This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: **http://www.theblackvault.com**

U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

July 5, 2018

MR. JOHN GREENEWALD JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1408601-000
Subject: Carnivore

Dear Mr. Greenewald:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act (FOIA). Below you will find informational paragraphs relevant to your request. Please read each item carefully.

Enclosed are 605 pages of previously processed documents and a copy of the Explanation of Exemptions. This release is being provided to you at no charge.

Please be advised that additional records potentially responsive to your subject may exist. If this release of previously processed material does not satisfy your information needs for this request, you may request an additional search for records. Submit your request by mail or fax to – Work Process Unit, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997. Please cite the FOIPA Request Number in your correspondence.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Sincerely,

David M. Hardy
Section Chief,
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF GENERAL COUNSEL
FRONT OFFICE
(THROUGH 7/28/00)

PAGES REVIEWED: 154

PAGES RELEASED: 154

EXEMPTIONS CITED: b6-1, b7C-1,
b6-3 & b7C-3

THE WALL STREET JOURNAL

DATE: 7/12/00

PAGE: B-11

Internet Companies Decry FBI's E-Mail Wiretap Plan

By Nick Wingfield
And Don Clark
Staff Reporters of The Wall Street Journal

Internet-service providers and privacy advocates are concerned about the implications of a new electronic surveillance system devised by the Federal Bureau of Investigation, with some providers vowing to resist if they are asked to install it on their networks.

The FBI system, a sophisticated combination of hardware and software the agency has dubbed Carnivore, must be connected directly to an ISP's network. Once it is connected, Carnivore has the potential to keep tabs on all of the communications on the network. The FBI has said it will use the system only with valid court orders and that Carnivore will allow it to narrowly target its investigations.

However, ISPs, industry representatives and privacy advocates, responding to a report in The Wall Street Journal about the FBI system, criticized the potential for excessive monitoring of online communications. "We have some deep concerns as we look at this harder," said Jeff Richards, executive director of the Internet Alliance, a trade association for Internet providers that counts America Online Inc., EarthLink Inc. and WorldCom Inc.'s UUNET division among its members.

The Carnivore system is believed to be able to single out all sorts of electronic traffic of a person being investigated. Besides e-mail, that includes instant-messaging systems, visits to Web sites and Internet relay chat sessions, a form of communication favored by hackers trying to mask their identities.

It isn't clear, however, whether Carnivore can overcome some of the sophisticated scrambling systems that have been developed for the Internet. Scrambling data to make it hard to read is an obvious response for people worried about their messages being caught up in the FBI vacuum cleaner. Such data-scrambling wouldn't necessarily prevent the FBI from knowing the message's destination, security experts said.

To better protect their cyber-trails, users would have to seek services designed to protect anonymity on the Internet. For example, Zero-Knowledge Systems, Montreal, sells users online pseudonyms for use when conducting business online.

Critics of the FBI system fear Internet-service providers will have little guarantee that Carnivore is doing only what the FBI says it is doing. Because the FBI seems to need little assistance in running the system, technicians for the ISPs can't do much to monitor whether FBI agents are limiting their investigations to an individual named in a court order.

"The FBI takes the position of, 'Trust us, we're the government. Open your entire network to us,' " says Barry Steinhardt, associate director for the American Civil Liberties Union, which sent a critical letter about Carnivore to members of Congress. "There's no way for an ISP to know what they're doing."

One ISP that hadn't been contacted by the FBI about Carnivore said it normally complies with court orders from law-enforcement agencies for the communications of specific individuals. But the ISP said it wouldn't comply with an order to install Carnivore on its network.

"I would have to say we would fight such a court order," said Ehud Gavron, the chief technology officer of RMI.Net Inc., an ISP based in Denver with 110,000 subscribers. "We would not want the privacy of all users to be compromised on the basis of witch hunts for one user."

The FBI argues that state and federal judges closely scrutinize its wiretapping activities and that the product of any telephone or Internet intercept must be open to outside audit. The bureau says that it developed the Carnivore system precisely to address the same privacy concerns that many Internet providers have. FBI technicians also have tried in recent weeks to explain to industry specialists how Carnivore works, partly to allay fears that the system might be open to abuse.

Still, there is a drive afoot in the Internet industry to create a more open solution that could replace Carnivore. Industry experts argue that creating their own device would lessen suspicions and allow for quicker modifications as Internet protocols change. The FBI says that a small number of Internet providers already have built-in capacities to meet federal wiretap requests. Carnivore is required for those that don't have the ability to do the wiretaps themselves.

—Neil King Jr. contributed to this article.

Journal Link: Read an issue briefing and join a discussion about privacy and the Internet in the online Journal at **WSJ.com**.

The Washington Post

DATE: 7-12-00

PAGE: E-1

FBI Internet Wiretaps Raise Issues Of Privacy

New System Tracks Suspects Online

By John Schwartz
Washington Post Staff Writer

The FBI has deployed an automated system to wiretap the Internet, giving authorities a new tool to police cyberspace but drawing concerns among civil libertarians and privacy advocates about how it might be used.

The new computer system, dubbed "Carnivore" inside the FBI because it rapidly finds the "meat" in vast amounts of data, was developed at FBI computer labs in Quantico, Va., and has been used in fewer than 50 cases so far.

But that number is sure to rise, said Marcus Thomas, chief of the FBI's cyber-technology section at Quantico. "In criminal situations there's not yet been a large call for it," he said, but the bureau already has seen "growth in the rate of requests."

Civil liberties groups said the new system raises troubling issues about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, the new technology also could scan private information about legal activities.

"It goes to the heart of how the Fourth Amendment and the federal wiretap statute are going to be applied in the Internet age," said Marc Rotenberg, head of the Washington-based Electronic Privacy Information Center.

The new system, which operates on off-the-shelf personal computers, takes advantage of one of the fundamental principles of the Internet: that virtually all such communications are broken up into "packets," or uniform chunks of data. Computers on the Internet break up e-mail messages, World Wide Web site traffic and other information into pieces and route the packets across the global network, where they are reassembled on the other end.

FBI programmers devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

The ability to distinguish between packets allows law enforcement officials to tailor their searches so that, for example, they can examine e-mail but leave alone a suspect's online shopping activities. The system could be tuned to do as little as monitoring how many e-mail messages the suspect sends and to whom they are addressed—the equivalent of a telephone "pen register," which takes down telephone numbers being called without grabbing the content of those calls.

"That's the good news," said James Dempsey, an analyst with the Center for Democracy and Technology, a Washington high-tech policy group. "It is a more discriminating device" than a full wiretap, he said.

But Dempsey expressed worries about the new system, which would be installed at the offices of a suspect's Internet service provider. Just as the device could be used to fine-tune a search, it also could used for broad sweeps of data. "The bad news is that it's a black box the government wants to insert into the premises of a service provider. Nobody knows that it does what the government claims it would do," Dempsey said.

Existence of the Carnivore system was discussed in a Wall Street Journal article yesterday, which reported that the FBI showed the system to telecommunications industry experts two weeks ago.

Albert Gidari, a lawyer who works for the wireless industry, was present at the FBI demonstration. He said the FBI's announcement was intended to counter industry assertions that it would be very difficult to provide the kind of pen-register wiretap capability that the agency wants.

Since the demonstration, Gidari said, one faction within the telecommunications industry was pleased with the FBI's efforts. But Gidari said the other faction was saying: "Wait a minute—what are the liability issues? What are the privacy issues? We don't want third-party software on our system."

Although Congress has passed legislation requiring telephone companies to make their developing high-tech networks easy to wiretap, Gidari is one of a large number of industry experts who believe the law does not apply to wiretapping the Internet. "The FBI overreaches in everything they do," said Gidari, who is president of G-Savvy, an Internet consulting company.

A former federal prosecutor sounded a more supportive tone. "If what it does is it helps comply with wiretaps, and it helps minimize what you're getting—to help get what the court authorizes you to get—there's nothing wrong with it," said Mark Rasch, now a security consultant with Reston-based Global Integrity.

Still, Rasch said the technology raised questions that have yet to be fully explored by law enforcement. The PC robocop examines all packets coming through a computer network but gives live law enforcement officers only those packets related to the subject of the investigation.

"The stuff that is examined only by a computer and not by a human being—was that information searched?" Rasch asked. He then suggested an answer: "It is a search, but it is to an extent less invasive than it would be if you did not use this technology."

The first news of Carnivore actually came in April during congressional testimony by Washington lawyer Robert Corn-Revere, who represented an Internet service provider that tried to resist attaching the system to its network. Corn-Revere suggested that such a system could be used to track dissidents and journalists online. "There are some human rights issues here," he said.

But Thomas of the FBI said there is nothing mysterious about the new device. "This is an effort on the FBI's part to keep pace with changes in technology—to maintain our ability" to lawfully intercept everything from pen-register data to full wiretaps with court authorization. "It's not an increase in our authority; it doesn't present a change of volume in what we do," he said.

DOC #2

Los Angeles Times

DATE: 7-14-
PAGE: A-16

Justice, on Both Sides of the Border

Agustin Vazquez Mendoza landed on the FBI's 10 most wanted list four years ago for allegedly ordering his henchmen to kill a Drug Enforcement Administration agent in Arizona. Now he's under arrest, but in Mexico, which must decide whether to extradite a Mexican citizen to face charges in the United States. Mexican law officers mounted a nationwide manhunt to capture Vazquez and certainly want him brought to justice, but some traffickers have won appeals against extradition.

Most countries are understandably reluctant to hand over a citizen to be tried in a foreign country. In addition, the language in the current Mexico-U.S. treaties clearly specifies that neither country is bound to extradite a citizen. However, there are circumstances in the Vazquez case that should make it easier for Mexico to send him off.

Since President Ernesto Zedillo took office, there has been a shift of attitude in Mexico on extradition. At least nine Mexican suspects have been sent to be tried in the United States. In two of those cases, the suspects allegedly killed U.S. immigration officials, inviting comparison with the Vazquez case.

According to U.S. authorities, Vazquez ordered the murder of agent Richard Fass in order to keep both a drug delivery and the $160,000 the undercover agent was about to pay for it.

Perhaps the most persuasive argument is that Vazquez, who fled to Mexico after the killing, is not accused of a crime in Mexico and if he is not extradited will have to be set free. Mexico's foreign minister should consent to the U.S. extradition request and petition the justice system to send him north as quickly as the legal process allows.

46

DOC. #3

THE WALL STREET JOURNAL

DATE: 7/14/02
PAGE: A16

EarthLink Says It Won't Install Device for FBI

One of the nation's largest Internet service providers, EarthLink Inc., has refused to install a new Federal Bureau of Investigation electronic surveillance device on its network, saying technical adjustments required to use the device caused disruptions for customers.

The FBI has used Carnivore, as the surveillance device is called, in a number of criminal investigations. But EarthLink is the first ISP to offer a public account of an actual experience with Carnivore. The FBI has claimed that Carnivore won't interfere with an ISP's operations.

By Wall Street Journal staff reporters Nick Wingfield, Ted Bridis and Neil King Jr.

"It has the potential to hurt our network, to bring pieces of it down," Steve Dougherty, EarthLink's director of technology acquisition, said of Carnivore. "It could impact thousands of people."

While EarthLink executives said they would continue to work with authorities in criminal investigations, they vowed not to allow the FBI to install Carnivore on the company's network. The company also has substantial privacy concerns.

EarthLink has already voiced its concerns in court. The ISP is the plaintiff in a legal fight launched against Carnivore earlier this year with the help of attorney Robert Corn-Revere, according to people close to the case. Previously, the identity of the plaintiff in the case, which is under seal, wasn't known. A federal magistrate ruled against EarthLink in the case early this year, forcing it to give the FBI access to its system. Mr. Corn-Revere declined to comment.

EarthLink's problems with Carnivore began earlier this year, when the FBI installed a Carnivore device on its network at a hub site in Pasadena, Calif. The FBI had a court order that allowed it to install the equipment as part of a criminal investigation.

The FBI connected Carnivore, a small computer box loaded with sophisticated software for monitoring e-mail and other online communications, to EarthLink's remote access servers, a set of networking equipment that answers incoming modem calls from customers. But Carnivore wasn't compatible with the operating system software on the remote access servers. So EarthLink had to install an older version of the system software that would work with Carnivore, according to Mr. Dougherty.

EarthLink says the older version of the software caused its remote access servers to crash, which in turn knocked out access for a number of its customers. Mr. Dougherty declined to specify how many, saying only that "many" people were affected.

EarthLink executives said they were also concerned about privacy. The company said it had no way of knowing whether Carnivore was limiting its surveillance to the criminal investigation at hand, or was trolling more broadly. Other ISPs have said there could be serious liability issues for them if the privacy of individuals not connected to an investigation is compromised.

"There ought to be some transparency to the methods and tools that law enforcement is using to search-and-seize communications," said John R. LoGalbo, vice president of public policy at PSINet Inc., an ISP in Ashburn, Va.

EarthLink executives declined to say whether the company has received court orders for information about other customers since the disruption earlier this year. EarthLink said it would help authorities in criminal investigations using techniques other than Carnivore.

The FBI insists that Carnivore doesn't affect the performance or stability of an Internet provider's existing networks. The bureau says Carnivore passively monitors traffic, recording only information that is relevant to FBI investigations.

In some cases, the FBI said, the Internet provider is equipped to turn over data without the use of Carnivore. This is common in cases where only e-mail messages are sought because that type of data can easily be obtained through less-intrusive means.

Attorney General Janet Reno said yesterday that she was putting the system under review. She said the Justice Department would investigate Carnivore's constitutional implications and make sure that the FBI was using it in "a consistent and balanced way."

47

Doc. #4

Parkinson
Ken
from: John E. Collingwood

White House Proposes Wiretap Law

By KALPANA SRINIVASAN
.c The Associated Press

WASHINGTON (July 17) - The White House proposed legislation Monday to update wiretapping rules so that legal protections currently applied to telephone calls are extended to electronic communication, such as e-mail.

The plan would require law enforcement officials to obtain high-level approval before applying for a court order to intercept the content of e-mail - in line with current rules that govern listening to phone calls.

"Basically, the same communication, if sent different ways - through a phone call or a dial-up modem - is subject to different and inconsistent privacy standards," said White House Chief of Staff John Podesta, in announcing the proposals. "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations."

The measure also addresses so-called "trap and trace" orders which allow law enforcement officials to identify the source of a phone call or an e-mail, but not intercept its content. Under the proposal, law enforcement officials would only need one order to trace an e-mail or a phone call, even though such communications may travel through multiple phone carriers or Internet providers.

Officials also could trace such communications without prior approval in an emergency situation, such as when a computer is under attack.

But for the first time, the administration is proposing that a federal or state judge independently determine whether the facts support such a trace order. Under current rules, judges accept the declaration of law enforcement officials agencies that such an order is warranted.

Those changes could affect the new "Carnivore" system, which the FBI is using to obtain e-mails of investigative subjects after getting a search warrant. When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

Under the proposed changes, if the Carnivore system is being used to intercept the content of electronic communications, then law enforcement officials would first need high-level Justice Department approval before obtaining a court order, Podesta said. Higher standards limiting its use also would apply, he said. If Carnivore is being used only to track information, officials would need an independent judge to review the tracing order, he added.

But the American Civil Liberties Union chided the administration's proposals Monday, saying it should have suspended use of the system outright.

"Carnivore represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic," said Barry Steinhardt, ACLU associate director.

Last week, ACLU officials said they were going to use the Freedom of Information Act to try to force the FBI to disclose details of the inner workings of Carnivore.

The proposed measures would also address inconsistencies in how current law applies to different networks carrying Internet traffic. For example, now that cable systems are being upgraded to offer two-way services, laws that apply to dial-up modems over phone lines should be extended to cable connections, Podesta said.

The proposal requires congressional approval, and several lawmakers already have introduced their own versions.

The Clinton administration also announced Monday updates to its export control policy for powerful data and voice-scrambling technology. Under the change, American companies can sell encryption products to any end user in the European Union or these eight other trading partners: Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The policy change will also remove a previous technical review waiting period of 30 days.

AP-NY-07-17-00 1458EDT

Doc #5

WALL STREET JOURNAL

DATE 7/17/00
PAGE B7

ACLU Asks Details On FBI's New Plan To Monitor the Web

By Nick Wingfield
Staff Reporter of The Wall Street Journal

The American Civil Liberties Union is seeking to force the Federal Bureau of Investigation to disclose the technical details behind a controversial electronic surveillance system created by the bureau.

The ACLU, using a novel tactic to identify the monitoring capabilities of the system, filed a Freedom of Information Act request with the FBI Friday, asking the bureau to release the computer "source code" for Carnivore, as the surveillance system is called. The civil-liberties group also requested that the FBI turn over "letters, correspondence, tape recordings, notes, data, memoranda, e-mail" and other information connected with Carnivore. The ACLU also asked for information related to Omnivore and EtherPeek, two other surveillance systems used in the past by the bureau.

The request reflects the growing concern among privacy groups and Internet companies about the privacy implications of Carnivore. The FBI surveillance system, a hardware device that contains a specialized program for tracking e-mail and other forms of online communication, has especially raised hackles among Internet service providers. The FBI is attempting to install Carnivore on the networks of ISPs as part of specific criminal investigations of online users. But ISPs say they have no way of knowing whether Carnivore is limiting the scope of its surveillance to the cases at hand.

As a result, critics of Carnivore have called on the government to reveal the technical capabilities of the system. Such information could indicate whether Carnivore is able to restrict its monitoring to the communications of, say, a single criminal suspect while ignoring other data traffic irrelevant to the investigation.

The source code behind Carnivore could provide clues to those capabilities. Source code is essentially the technical blueprint behind a program. The ACLU contends, and technical experts concurred, that examining the source code behind Carnivore's proprietary surveillance software could reveal something of the inner workings of the system.

The Electronic Privacy Information Center, a Washington advocacy group, last week also filed a sweeping Freedom of Information request for "all records" relating to Carnivore, though it didn't explicitly request the system's source code. "But we made clear we are seeking everything, including software," said David Sobel, a privacy activist at the center.

It is unclear whether using the Freedom of Information Act will compel the FBI to produce the software behind Carnivore though. Requests made under the act are normally used to obtain official government documents, not software code. Barry Steinhardt, associate director of the ACLU, said two federal appeals-court rulings that classified software code as a form of speech could help his case.

"I am all but certain they will not want to release any information on Carnivore, and we will probably have to fight this in the courts," Mr. Steinhardt said of the FBI. "But we think this is worth fighting for."

The FBI didn't return calls seeking comment on the Freedom of Information request.

As the outcry against Carnivore has escalated, some prominent figures in the Internet industry have expressed a somewhat more sympathetic view toward the FBI. Vint Cerf, who has been dubbed the "father of the Internet" for his development of the early technical foundations of the network, said it is "understandable that law-enforcement agencies feel pressed to develop methods to observe Internet traffic for the same reasons they have felt compelled to find ways to listen to certain telephone conversations."

But Mr. Cerf, in an e-mail message, added that such modern surveillance techniques need to be balanced "against potentially abusive practices that could seriously erode personal privacy"

—Neil King Jr. contributed to this article.

Coca-Cola Files to Have Second Race-Bias Suit Moved to Federal Court

By a Wall Street Journal Staff Reporter

ATLANTA—Coca-Cola Co., in the process of settling a class-action race-discrimination lawsuit, has filed a motion to move a second, $1.5 billion race-bias suit to federal from state court.

The soft-drink company argued in a motion filed Friday that most of the claims in the lawsuit, filed last month on behalf of four female black Coke employees by Willie E. Gary and Johnnie Cochran, involve federal laws.

But a lawyer on Mr. Gary's team, Tricia C.K. Hoffler, disagreed and said Mr. Gary would file a motion this week to keep the case in state court. Mr. Gary, a personal-injury attorney, generally brings his cases to state courts and has said he prefers that venue.

The lawsuit filed by Mr. Gary claims a variety of forms of discrimination, including negligent hiring, intentional infliction of emotional harm and hostile work environment. Coke has called Mr. Gary an opportunist and denied the charges.

Doc. #6

WASHINGTON

DATE 5/24/02
PAGE E1

U.S. Hopes to Extend Online Wiretapping

By John Schwartz
Washington Post Staff Writer

The Clinton administration yesterday called for updating wiretapping laws to extend the powers of law enforcement to the online world while providing new legal protections for electronic communication.

Administration officials also announced, as expected, a plan to loosen controls on the export of encryption software—the programs that help Internet users scramble messages and data to protect them from prying eyes.

On the wiretapping issue, White House chief of staff John D. Podesta, in a speech at the National Press Club, described the coming legislative package as seeking to eliminate confusion about the level of legal protection for various forms of communication.

Telephone conversations get fairly strong protection from federal wiretaps under the 1968 Crime Patrol and Safe Streets Act, which required a court order and high-level Justice Department approval. Wiretape rules for e-mail sent by dial-up modem are covered by the Electronic Communications Privacy Act of 1986. That law might not cover e-mail sent by high-speed cable modem, and cable companies have argued that their online services should be given extremely high protection from government surveillance under the Cable Act.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Podesta said.

Lawmakers said they welcome the opportunity to work with the administration on these issues. Sen. Orrin G. Hatch (R-Utah), who has introduced an Internet privacy bill, said: "It is imperative that we balance the interests of law enforcement with the privacy rights of the American people. We must ensure that appropriate checks are in place where the government accesses private communications of Americans."

Podesta said the bills making up the package would be unveiled within 10 days, and that he hopes the legislation can be passed by the end of the year.

Podesta also spoke about the new surveillance technology known as Carnivore, which gives law enforcement authorities the ability to selectively monitor the Internet traffic of individuals, similar to the devices that can record the telephone numbers of calls made and received by a suspect. Unlike full-fledged wiretaps, the judicial oversight of such surveillance is slight, and the protection against abuses of the technology by law enforcement is weak. Podesta called for greater judicial oversight.

The Podesta speech was not well received by civil liberties advocates, who have fought Carnivore and other administration attempts to expand wiretapping capabilities on the Internet. Barry Steinhardt, associate director of the American Civil Liberties Union, called the speech "deeply disappointing. . . . While the Clinton administration's proposals have some heartening qualities to them, they are too little and too late," with too little time in the legislative session to pass new bills. The Carnivore system, Steinhardt said, "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic."

Podesta also discussed the new encryption policy, which the administration can implement immediately. Under the plan, U.S. companies will be able to export sophisticated cryptography products to users in any nation in the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The government will eliminate the statutory 30-day waiting period before such exports can take place but will keep in place a requirement that new technologies be submitted to the government for a technical review.

Encryption has been a high-tech battlefield from the early days of the Clinton administration. Few technologies are as important in the fight to maintain personal and business privacy, but few technologies present such daunting issues for law enforcement officials like FBI Director Louis J. Freeh, who often warns that criminals and terrorists can use "crypto" to cloak their plans and activities. High-tech companies successfully argued that U.S. restrictions harmed only American companies, since overseas firms were successfully marketing strong encryption products, and in January the Clinton administration reduced controls on encryption exports.

"The reducing of these regulations will certainly allow U.S. software makers to compete in the global marketplace," said Robert Holleyman, the chief executive of the Business Software Alliance.

Doc #7

WALL STREET JOURNAL

DATE 7/19/00
PAGE A22

'Carnivore' Won't Devour Cyber-Privacy

By Bruce Berkowitz

On Monday the White House proposed new legislation regulating surveillance by law enforcement agencies on the Internet. But civil libertarians are already complaining that this plan does little to address the problems ostensibly raised by Carnivore, the FBI's new software system for performing court-ordered wiretaps at Internet service providers (ISPs).

Using a laptop computer, law enforcement officials can hook Carnivore into an ISP's network. Once installed, it reads the headers of each e-mail message—listing the sender, recipient and subject of the message—as it passes through. If the sender or recipient is the target of a tap, Carnivore records the message.

Rights at Risk?

Here's the rub: Before Carnivore can know whether a message belongs to a targeted party, it must browse the headers of all the messages passing through the ISP. With a traditional phone tap, law enforcement officers only listened to the telephone line that the subject of the tap was using. The ACLU and other critics complain that when Carnivore reads the headers of anyone who is not a target it violates their rights.

The ACLU and other Carnivore critics need to get a grip—and a better understanding of the new technology.

Unlike old-fashioned analog telephone calls, e-mail messages are transmitted digitally. A computer slices and dices the message into packets, each with an identifying tag. The packets then spread out throughout the Internet, finding the most efficient path to the destination. When they arrive, they are reassembled, and the recipient gets the message. As a result, with e-mail, you cannot "tap a line" because often there is, literally, no particular line to tap. All you can do is scan the messages that pass through a link a suspect is known to use—like his ISP—and pick out the ones that belong to him. That's what Carnivore does.

The ACLU complains that using a computer to monitor an ISP system would collect vast amounts of innocent data. But what do they expect the feds to use—a typewriter and an abacus? Note to FBI: Hire a better public relations firm, and name your next project "Vegetarian."

These kinds of flaps are happening more and more often. Last April some privacy advocates complained when the FBI requested $15 million for "Digital Storm," a program for monitoring telephone calls and analyzing recordings. In September, a programmer in North Carolina found the notation "NSA Key" in a Microsoft software patch. Soon rumors bounced through the Internet claiming Windows had a back door that allows the National Security Agency to monitor your computer. (Microsoft explained that the tag merely signified that the software complied with the agency's security standards.)

The granddaddy of all bogus fears, though, is Echelon. If you believe some European Union parliamentarians, the United States and Britain operate an international network that monitors virtually all communications, and extracts choice nuggets with powerful computers that recognize key phrases in messages like "assassination," "terrorist attack" or "industrial secret."

In reality, it's not easy to find a specific message in a flood of free-flowing digital data. That's the whole reason for getting a court order for a wire tap. If you cannot hook into an ISP, you have to do a lot of searching to find the message you want to intercept.

That is also why the European campaign against Echelon is so quixotic. True, the folks at NSA intercept communications and they have powerful computers and ingenious software that helps with the processing. But it is impossible for even the best computer system to routinely sort through all of the world's telecommunications and pull out telltale messages, as the Echelon paranoids would have you believe.

Usually you need to know what you are looking for and where the message might appear before you have much of a chance of finding it. Also, the cases in which one message tells a whole story are rare. Good law enforcement and intelligence usually requires multiple sources and collateral information to make sense of an intercept.

The privacy advocates have the story reversed. It's getting harder, not easier, for our law enforcement and intelligence organizations to listen in on communications. In the old days you could tap a line or intercept a microwave link. It's much more difficult to capture digital messages that pass over fiber optics or bounce through cellular networks. And, with strong encryption software freely available world-wide, anyone really determined to keep a message secret can usually do so.

If you have any doubts, just recall how many intelligence surprises we have had lately—the Indian nuclear test, the North Korean missile test, the terrorist bombings of American targets in the Mideast and Africa. Part of the problem is that we cannot get to many of the sources that we used to, and everyone is getting better at concealing their communications.

So why is it so easy to stir up these controversies about privacy? The simple fact is that relations between the government and the new information industries are lousy. There is too much suspicion and too little communication.

The administration gets part of the blame for its ham-handed policies. Carnivore is a good example. A lot of controversy could have been defused if the FBI had offered more insight into how the system worked and how the rights of non-suspects would be protected.

But the record of the technogeeks has not been much better. They often act as though law enforcement officials have no business poking into their activities at all—as though one could stop international computer criminals with a good neighborhood watch program.

It's all too easy to lose sight of the fact that Carnivore's main targets are cyber-criminals—in other words, the kinds of crooks who are a plague on the Internet and target dot-com companies. Growth rates for Internet shopping have been slipping lately. According to some experts, people worry about whether their credit card numbers and health records are safe. You would think that e-business would be the first to support better law enforcement on the net.

Common Goals

All the good guys in this dispute have common goals. Defense and intelligence officials want to protect the nation's communications infrastructure. Law enforcement officials want to chase crooks, and companies want the cops to catch them. Consumers want privacy. The path to all is the same: secure information systems.

Doc. #8

2

reasonable cooperation from the private sector, and aggressive law enforcement and effective intelligence closely monitored by responsible public officials.

Fixing the relationship between Washington and Silicon Valley needs to be a top priority for the next administration. The only people benefitting from controversies like the one over Carnivore are terrorists, criminals and rogue states.

Mr. Berkowitz is a research fellow at the Hoover Institution and coauthor of "Best Truth: Intelligence in the Information Age" (Yale University Press, 2000).

July 19, 2000

Honorable Charles T. Canady
Chairman
Subcommittee on the Constitution
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

We very much appreciate the opportunity to appear before the Constitution Subcommittee on Monday to discuss "Carnivore." The public testimony, we believe, will be very helpful in our efforts to explain what Carnivore is and, equally important, what it is not.

In that regard, *USA Today* asked us to provide a brief 350 word explanation for use on the editorial page. While a full statement obviously will be provided to the Subcommittee, we would like to share with you the text of what was provided to the newspaper. In a very concise fashion, it encapsulates our explanation of what the system does electronically to ensure strict compliance with the court orders that instruct us precisely what can and cannot be intercepted. I also have enclosed a graphic that you may find helpful.

As the brief summary points out, Carnivore is used only when Internet Service Providers are unable on their own to restrict interceptions within the narrow confines of the controlling court order. In addition, no interception can occur unless the FBI or other law enforcement agency can demonstrate to a judge's satisfaction that the strict statutory requirements have been met, e.g., that there is probable cause that a crime is being or has been committed, that the intercepted e-mails will be in furtherance or about that crime, and that the interceptions are necessary to collect evidence of that crime. That is why its use has been very limited, predominately to intercept e-mails in terrorism cases.

I hope you find this helpful. Again, we look forward to testifying and, in the interim, if you have any questions, please do not hesitate to ask. We would be pleased to brief on any aspect of this system.

Sincerely yours,

John E. Collingwood
Assistant Director
Office of Public and
Congressional Affairs

1 - Mr. Pickard - Rm 7142
1 - Mr. Alba - Rm 7128
1 - Mr. Gallagher - Rm 7110
1 - Mr. Garcia - Rm 7116
1 - Dr. Kerr - Rm 3090
1 - Mr. Parkinson - Rm 7427
1 - [redacted] - Rm [redacted]
JEC:mmc (25)

1 - Mr. Collingwood
1 - [redacted] 66-1
1 - [redacted] 67C-1
1 - CAO file copy

IDENTICAL LETTERS SENT TO ALL
ADDRESSES ON ATTACHED LIST

Doc. #9

Honorable Charles T. Canady

Honorable Henry J. Hyde
House of Representatives
Washington, D.C. 20515

Honorable Asa Hutchinson
House of Representatives
Washington, D.C. 20515

Honorable Spencer Bachus
House of Representatives
Washington, D.C. 20515

Honorable Robert W. Goodlatte
House of Representatives
Washington, D.C. 20515

Honorable Bob Barr
House of Representatives
Washington, D.C. 20515

Honorable William L. Jenkins
House of Representatives
Washington, D.C. 20515

Honorable Lindsey Graham
House of Representatives
Washington, D.C. 20515

Honorable Melvin L. Watt
House of Representatives
Washington, D.C. 20515

Honorable Maxine Waters
House of Representatives
Washington, D.C. 20515

Honorable Charles T. Canady

Honorable Barney Frank
House of Representatives
Washington, D.C. 20515

Honorable John Conyers, Jr.
House of Representatives
Washington, D.C. 20515

Honorable Jerrold Nadler
House of Representatives
Washington, D.C. 20515

5/24/02 Release - Page 12

First, lets get the facts straight. The FBI and all other law enforcement agencies can only intercept e-mails pursuant to a court order signed by a judge who is satisfied that the government has demonstrated probable cause that a serious crime is being or has been committed, the e-mails will be about that crime and the interception is necessary to obtain evidence about the crime. To conduct an intercept beyond that is a federal crime subject to severe criminal and civil sanctions. The entire process requires continual reporting to a court and, of course, ultimately is subject to vigorous challenge by defense attorneys.

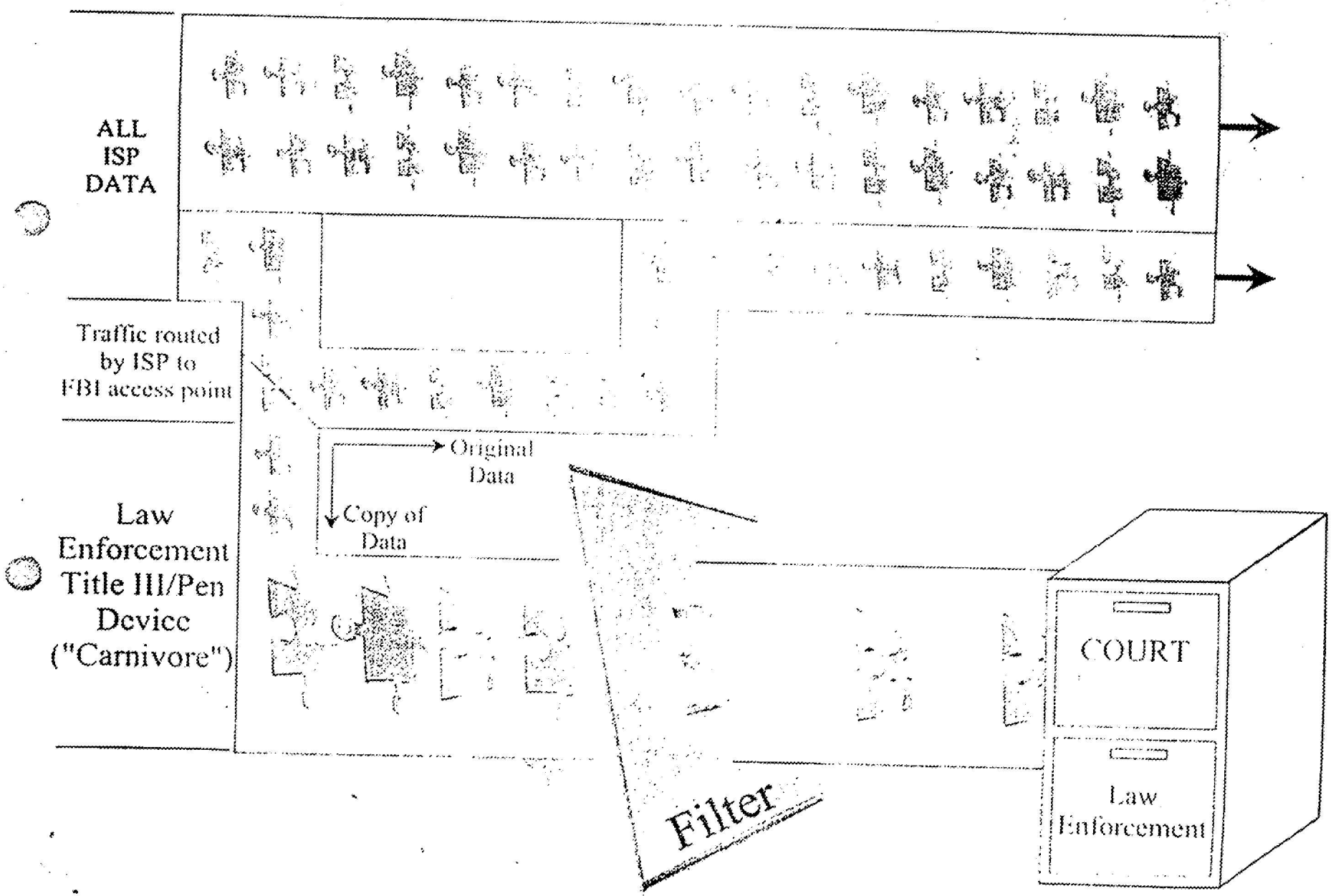
What does "carnivore" do? In the simplest terms, it ensures that only the exact communications authorized by the court to be intercepted are what is intercepted. So, for example, if a court authorizes only the interception of e-mail from a particular drug dealer to another drug dealer, this system captures only that e-mail to the exclusion of all other computer communications regardless of who sends them and where they are going. Nothing else is monitored or collected, and everything collected is supervised by the court. It would be a federal crime to do otherwise.

When is carnivore used? It is used only when an Internet service provider cannot, on its own, effect the interceptions consistent with a narrow court order. Accordingly, it has been used very few times, predominately to intercept e-mails in terrorism cases and, again, subject to the supervision of a court.

In 1968, Congress spelled out strict requirements for the interception of communications. Carnivore simply ensures that law enforcement complies precisely with those requirements as technology advances. We understand why certain segments oppose this court ordered technique. But since 1968, because of this law, many lives have been saved and thousands of drug dealers, terrorists, child predators and spies are in jail.

The Chairman of PSINet laid out the appropriate challenge. He does not want to see carnivore on his network unless we can prove it sifts out only the traffic from the target of a court order. That, of course, is precisely what carnivore does, electronically protecting the privacy of those not subject to the court order.

5/24/02 Release - Page 15



WALL STREET JOURNAL

DATE 7/20/00
PAGE A28

Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI

By Ted Bridis
And Neil King Jr.
Staff Reporters of The Wall Street Journal

WASHINGTON—Packed in a slim laptop computer, the Federal Bureau of Investigation's Internet surveillance system, Carnivore, looks downright docile. One of its creators calls it merely a "tool in a tool box" for tracking hackers and terrorists. Its name, the FBI admits, is unfortunate.

It is too late to change the name—but not too late, the FBI figures, to try to change the opinions of privacy advocates and lawmakers who have spoken harshly of the high-tech sniffer. So the agency has launched an intense, behind-the-scenes campaign to deflect congressional skepticism and convince wary Internet companies that Carnivore is a much pickier eater than its critics claim.

Since news of Carnivore broke last week, FBI officials have swarmed Capitol Hill to demonstrate the system to key members of Congress and their staff. The officials also have shown it to two federal judges and a small group of reporters for The Wall Street Journal. And Tuesday, the FBI published a lengthy article about Carnivore on its Web site, describing it as a "diagnostic tool" that employs new technology "to lawfully obtain important information while providing enhanced privacy protection."

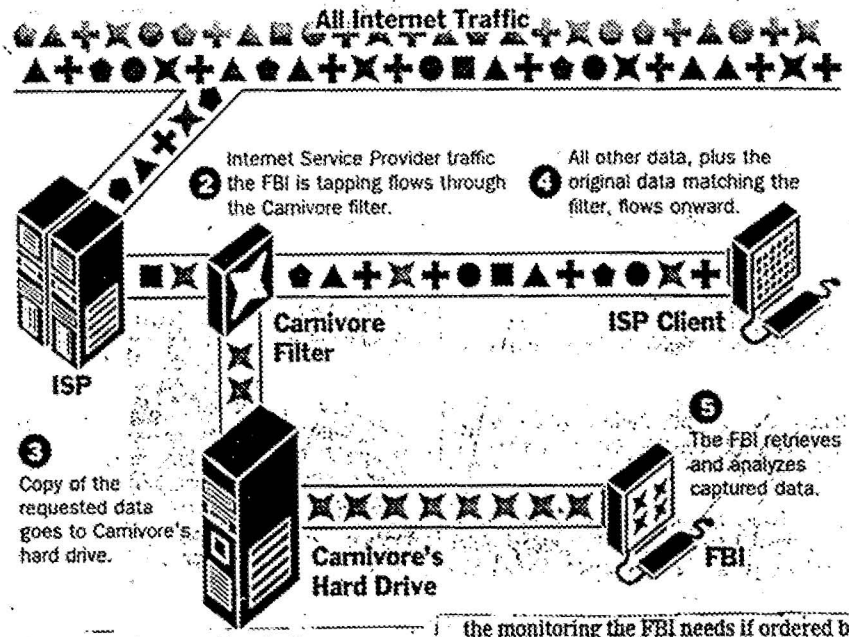
The message: Carnivore is a surgical law-enforcement device used rarely and only under strict court orders. And, contrary to fears espoused publicly in recent days, the system doesn't gobble up all passing e-mail in its search for the correspondence of a single suspect. "This device is blind to everything but the packet [of information] that it's set to retrieve," says Thomas Motta, an assistant general counsel for the FBI. "It's like a cop who can't see anything but a blue car on a highway."

In advance of a hastily called congressional hearing next week, FBI officials also have been expressing regrets about the system's name. Carnivore was the in-house moniker given to the successor of an earlier surveillance system, which was called Omnivore. No one thought the name would become public. When it did last week, Attorney General Janet Reno called for a name change, and FBI Director Louis Freeh started asking how the bureau could have had such a tin ear.

"Let's just say, we're going to put names through the giggle-test a little differently in the future," says Donald Kerr, director of the special Quantico, Va., lab that developed Carnivore.

The system's critics are likely to demand more than merely cosmetic change. Lawmakers are eager to know how voracious Carnivore could get. Can it vacuum up Internet communications from innocent users? How frequently is it used, and under what legal basis? Is Carnivore hooked permanently into the country's Internet service providers? How can we trust that it does only what the FBI says?

The Workings of Carnivore



Protecting Citizens

"We want to hear exactly how this system works and make sure it raises no constitutional problems," says Rep. Charles Canady, the Florida Republican who heads the House judiciary subcommittee that will question FBI officials next week. Adds Rep. Asa Hutchinson, an Arkansas Republican and member of the same panel: "We have to protect citizens from inadvertent action as well as snooping by the government."

The system is designed to allow the FBI to conduct efficient wiretaps of e-mail conversations and other online communications involving suspected hackers, terrorists and other criminals. The fear among critics is that Carnivore will scoop up transmissions made between innocent civilians and lay them open to scrutiny.

Internet providers, such as Iconn.Net of New Haven, Conn., say Carnivore is unnecessary because they already can do the monitoring the FBI needs if ordered by a court. "We're able to do it faster, more efficiently and, most importantly, without intruding on the privacy of people not within the scope of the search," says Peter William Sachs, president of Iconn.Net, who is scheduled to testify at next week's hearing. EarthLink Inc., one of the nation's largest Internet-service providers, says it refused earlier this year to install Carnivore on its network, claiming technical adjustments required to use the device caused disruptions for its customers.

In its meetings with lawmakers and others, the FBI has described the inner workings of the system in unusual detail. In one demonstration this week, the agency was keen to show how the system could tailor its search so it captures only the e-mails moving into and out of one particular account. The FBI said Carnivore is smart enough to capture a suspect's e-mails while leaving untouched messages sent by his or her spouse or children.

Doc. #10

'Packet Filters'

The system belongs to a class of tools known as "packet filters" or "sniffers," which look for parcels of data that travel across a network and comprise an e-mail or a visit to a Web site. Using a Windows screen, Carnivore also can be set to capture file downloads and chat-room conversations. It can grab e-mail from the most popular Web-based companies, including Yahoo! Inc. and Microsoft Corp.'s Hotmail. And once it is installed at an Internet service provider, the FBI can dial into Carnivore to make changes and monitor data that have been collected.

The FBI is adamant about dispelling fears that Carnivore could be used for rampant tapping of public e-mail systems. For one, wiretapping requests are closely scrutinized by the Justice Department, and must be approved by a federal judge. Abuse by a rogue investigator is even less likely, the bureau says, because the rogue would need too much cooperation from other FBI techies and the Internet service provider, says Marcus Thomas, a developer of the system at Quantico.

Depending on a judge's instructions, Carnivore can be set to merely trace Internet communications to and from a suspect, called a "pen register" or "trap and trace." Carnivore records the Internet addresses of passing traffic but not, for example, the contents or even the subject line of an e-mail. Since the amount of information gathered is relatively small in these instances, even a week's worth of monitoring can be stored on a single floppy disk, the agency says. With judicial permission, the system also can conduct fuller intercepts, which would gather the contents of the e-mails and other data.

The FBI says Carnivore doesn't monitor the content of passing e-mails, a capability widely rumored to exist in the controversial "Echelon" surveillance network operated overseas by the National Security Agency. Bureau officials said watching for key words in passing e-mails was technically possible, but that it would slow Internet traffic unacceptably for all customers. "If you attempt with a machine like this to actually read everything that goes by, you very quickly cannot deal with it," Mr. Thomas says.

The FBI now says it has used Carnivore in fewer than 25 investigations over the past 18 months, most targeting suspected terrorists or computer hackers. In each case, the system was connected to a commercial Internet service provider, where it intercepted data or e-mails in strict compliance with a court order, the FBI says.

Privacy advocates, who haven't been privy to the FBI demonstrations, hunger for much more than explanations. The American Civil Liberties Union wants the FBI to suspend Carnivore's use, arguing that Internet providers can already conduct adequate electronic wiretaps. The ACLU also has filed a request under the Freedom of Information Act for the blueprints of how Carnivore works. Many in the industry want these same plans—called the "source code"—to insure that the system isn't open to abuse and won't disrupt business.

The FBI says making Carnivore's inner workings public would allow hackers to defeat it. "Once you know how it works ... it could be fairly trivial to evade it," Mr. Thomas says.

Legislation to quash Carnivore entirely is unlikely, but lawmakers could move to tighten the requirements for its use or to impose rules that would further protect the privacy of innocent Internet users. Many argue that Carnivore points up the need for Congress to wrestle with a larger dilemma: updating the nation's wiretap laws, hatched long before the Internet existed.

2

From: [redacted] 6C-1/67C-1
To: CHARLES STEELE, DONALD KERR, LARRY PARKINSON, ...
Date: 7/20/00 4:38PM
Subject: DOJ review of statement.

Gentlemen:

Upon giving the "final" draft of Dr. Kerr's statement to OPCA, I was informed that DOJ will also review our final version of the statement before OPCA disseminates it to the Senate.

OPCA anticipates that DOJ will make recommendations to tweak the statement, therefore I'll revise the current FBI approved version with highlighted text of the DOJ recommendations for your review and comments before releasing it back to OPCA.

Dr. Kerr: This note is to confirm that 18 U.S.C. section 2511 does set forth the punishment for intentionally violating both Title III and ECPA.

[redacted] 6C-1
OGC/ILU 67C-1

DOC. #11

From: [redacted]
To:
Date: 7/20/00 6:20PM
Subject: Don Kerr's Testimony

b6-1
b7C-1

b6-1
b7C-1 [redacted]

The revisions that I just gave you do not include a fix for the problem that we just discussed, namely, the difference between T-III's standards for interception of oral/wire communications, and those for electronic communications. The former are set forth in 18 USC 2516(1), the latter in 18 USC 2516(3).

For the purpose of this testimony, the two main differences are:
(1) that applications under 2516(3) do not require senior level DOJ approval and (2) that they are not limited to "certain federal felonies. Thus if we strike the sentence at the bottom of page two/top of page three (referring to authorization by a senior official of DOJ) and the last sentence in the first paragraph of page three ("Further, interception of communications is limited to certain specified felony offenses.") we will remove some of the misleading inferences as to which provision we follow when seeking court approval to intercept e-mail. There may may be other instances where the testimony suggests that we use 2616(1) rather than 2516(3); OGC should scrub the testimony again to check for such instances.

b6-1
b7C-1 [redacted]

CC: [redacted] CHARLES STEELE [redacted]

b6-1
b7C-1

Doc #12

July 21, 2000

URGENT

Note for:

OLC
FBI [redacted] 6b-1 7c-1
OPD
EOUSA
ODAG [redacted] – did you get the FBI's statement from yesterday?) 6b-3 7c-3

From: [redacted] OLA 6b-3 7c-3

Re: CRM statement for 7/24 on "Carnivore" and the 4th amendment

Please provide comments (or "no comment") on the attached by 2 PM today, Friday.

Thanks.

cc: [redacted] OLA
6b-3
7c-3
Please provide c

Doc. #13

STATEMENT OF
KEVIN V. Di GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE
BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION
OF THE HOUSE COMMITTEE ON THE JUDICIARY
on
"CARNIVORE" AND THE FOURTH AMENDMENT

July 24, 2000

Mr. Chairman and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment. On April 6, 2000, I had the privilege of testifying before you during a hearing on Internet privacy and the Fourth Amendment; I am pleased to continue to participate in the discussion today about "Carnivore" and its role in protecting individual privacy on the Internet from unwarranted governmental intrusion, and about the critical role the Department plays to ensure that the Internet is a safe and secure place.

Privacy and Public Safety

It is beyond dispute that the Fourth Amendment protects the rights of Americans while they work and play on the Internet just as it does in the physical world. The goal is a long-honored and noble one: to preserve our privacy while protecting the safety of our citizens. Our founding fathers recognized that in order for our democratic society to remain safe and our liberty intact, law enforcement must have the ability to investigate, apprehend and prosecute people for criminal conduct. At the same time, however, our founding fathers held in disdain the government's disregard and abuse of privacy in England. The founders of this nation adopted the Fourth Amendment to address the tension that can at times arise between privacy and public

5/24/02 Release - Page 21

safety. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. The Electronic Communications Privacy Act ("ECPA") establishes a three-tier system by which the government can obtain stored information from electronic communication service providers. In general, the government needs a search warrant to obtain the content of unretrieved communications (like e-mail), a court order to obtain transactional records, and a subpoena to obtain information identifying the subscriber. *See* 18 U.S.C. §§ 2701-11.

In addition, in order to obtain source and destination information in real time, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. *See* 18 U.S.C. 1821 et. Seq.

Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510-22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.

The safeguards for privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement, clarifying what is acceptable evidence

gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in preserving privacy. When law enforcement investigates, successfully apprehends and prosecutes a criminal who has stolen a citizen's personal information from a computer system, for example, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emerging technologies that are changing the face of communications. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

Law Enforcement Tools in Cyberspace:

Although the Fourth Amendment is over two centuries old, the Internet as we know it is still in its infancy. The huge advances in the past ten years have changed forever the landscape of society, not just in America, but worldwide. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. As has been the case with every major technological advance in our history,

however, we are seeing individuals and groups use this technology to commit criminal acts. As Deputy Attorney General Eric Holder told the Crime Subcommittee of this Committee in February, our vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

To satisfy our obligations to the public to enforce the laws and preserve the safety, we use the same sorts of investigatory techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional, statutory, internal and court-ordered boundaries. Carnivore is simply an investigatory tool that is used online only under narrowly defined circumstances, and only when authorized by law, to meet our responsibilities to the public.

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling. To investigate this, it is helpful to determine who is communicating with the drug dealer. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager, and either the telephone company or law enforcement would have installed these devices to comply with the court's order. Thereafter, the source and destination of his phone calls would have been recorded. This is information that courts have held is not protected by any reasonable expectation of privacy. Given the personal nature of this information, however, the law requires government to obtain an order under these circumstances. In this way, privacy is protected and law enforcement is able to investigate to protect the public.

Now, that same drug dealer may be just as likely to send an e-mail as call his confederates. When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like Carnivore.

When a criminal uses e-mail to send a kidnaping demand, to buy and sell illegal drugs or to distribute child pornography, law enforcement needs to know to whom he is sending messages and from whom he receives them. To get this information, we obtain a court order, which we

serve on the appropriate service provider. Because of the nature of Internet communications, the addressing information (which does not include the content of the message) is often mixed in with a lot of other non-content data that we have no desire or authority to gather. If the service provider can comply with the order and provide us with only the addressing information required by court order, it will do so and we will not employ Carnivore. If, however, the service provider is unwilling or unable to comply with the order, we simply cannot give a criminal a free pass. It is for that narrow set of circumstances that the FBI designed "Carnivore."

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather only the email addresses of those persons with whom the drug dealer is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. In other words, Carnivore is a *minimization* tool that permits law enforcement strictly to comply with court orders, strongly to protect privacy, and effectively to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

As with any other investigative tools, there are many mechanisms we have in place to prevent against possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment, of course, restricts what law enforcement can do with Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act, and the courts.

For federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example,

before Carnivore may be used to intercept wire or electronic communications, the requesting investigatory agency must obtain approval from the Department of Justice. Specifically, the Office of Enforcement Operations in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. Similarly, typically the U.S. Attorney or the section chief within the Department who is handling the investigation also reviews the Title III intercept request. Even if the proposal clears the OEO, approval must be given by a Deputy Assistant Attorney General. Although this requirement of high-level review is required by Title III only with regard to proposed intercepts of wire and oral communications, the Department voluntarily imposes the same level of review for proposed interceptions of electronic communications (except digital-display pagers). Typically, investigative agencies such as the Federal Bureau of Investigation have similar internal requirements, separate and apart from Constitutional, statutory or Department of Justice requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be approved by the proper court. The court will evaluate the application under the Fourth Amendment and using the familiar standards of Title III. By statute, for example, the application to the court must show, through sworn affidavit, why the intercept is necessary as opposed to other less-intrusive investigatory techniques. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the

offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court.

Courts also often impose their own requirements. For example, many federal courts require that the investigators provide periodic reports setting forth information such as the number of communications intercepted, steps taken to minimize irrelevant traffic, and whether the interceptions have been fruitful. The court may, of course terminate the interception at any time.

The remedies for violating Title III or ECPA by improperly intercepting electronic communications can include criminal sanctions, civil suit, and for law enforcement agents, adverse employment action. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Carnivore itself also contains self-regulating features. For example, because of its sophisticated passive filtering features, it automates the process of minimization without intrusive monitoring by investigators, and simply disregards packets of information that do not satisfy the criteria in the court's authorization. Indeed, one of the most powerful privacy-protecting features of Carnivore is its ability to ignore information that is outside the scope of the court-ordered authority. For later verification, it also logs the filter settings. In addition, as a practical matter, Carnivore is not deployed except with close cooperation with the appropriate system provider. In any event, the FBI does not use Carnivore in every instance in which the court orders a Title III electronic communication intercept. Indeed, I understand that the Bureau uses Carnivore only in those instances when the service provider is unable to comply with the court order using its own equipment, or when the provider asks the FBI to use Bureau equipment.

As I testified in April, we face three major categories of challenges in trying to keep the Internet a safe and secure place for our citizens. These are:

1. Technical challenges that hamper law enforcement's ability to locate and prosecute criminals that operate online;
2. Certain substantive and procedural laws that have not kept pace with the changing technology, creating significant legal challenges to effective investigation and prosecution of crime in cyberspace; and
3. Resource needs that must be addressed to ensure that law enforcement can keep pace with changing technology and has the ability to hire and train people to fight cybercrime.

Carnivore is an investigative tool that assists us in meeting the first challenge. As we have witnessed, tracking a criminal online is not always an impossible task using our investigative tools. For example, last year federal and state law enforcement combined to successfully apprehend the creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California. Although we are proud of these important successes, we still face significant challenges as online criminals become more and more sophisticated.

In nearly every online case, tracking the online criminal requires law enforcement to attempt to trace the "electronic trail" from the victim back to the perpetrator. In effect, this "electronic trail" is the fingerprint of the twenty-first century – only much harder to find and not

as permanent as its more traditional predecessor. In the physical world, a criminal and his victim are generally in the same location. But cybercriminals do not have to physically visit the crime scene. Instead they cloak their illegal activity by weaving communications through a series of anonymous remailers, by creating forged e-mail headers with powerful point and click tools readily downloadable from hacker websites, by using a "free-trial" account or two, or by "wiping clean" the logging records that would be evidence of their activity.

In some cases, the criminal may not even be in the same country as the victim. The global nature of the Internet, while one of the greatest assets of the Internet to law-abiding citizens, allows criminals to conduct their illegal activity from across the globe. In these cases, the need to respond quickly and track the criminal is increasingly complicated and often frustrated by the fact that the activity takes place throughout different countries. With more than 190 countries connected to the Internet, it is easy to understand the coordination challenges that face law enforcement. Furthermore, in these cases, time is of the essence and the victim may not even realize they have been victimized until the criminal has long since signed-off. Clearly, the technical challenges for law enforcement are real and profound.

This fact was made clear in the findings and conclusions reached in the recently released report of the President's Working Group on Unlawful Conduct on the Internet, entitled, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." This extensive report highlights in detail the significant challenges facing law enforcement in cyberspace. As the report states, the needs and challenges confronting law enforcement, "are neither trivial nor theoretical." The Report outlines a three-pronged approach for responding to unlawful activity on the Internet:

1. Conduct on the Internet should be treated in the same manner as similar conduct offline, in a technology neutral manner.

2. We must recognize that the needs and challenges of law enforcement posed by the Internet are substantial, including our the need for resources, up-to date investigative tools and enhanced multi-jurisdictional cooperation.

3. Finally, continued support for private sector leadership in developing tools and methods to help Internet users to prevent and minimize the risks of unlawful conduct online.

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report can be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at www.cybercrime.gov. In addition to the report, www.cybercrime.gov also contains other useful information on a wide array of Internet related issues, including the topic of today's hearing – privacy.

Despite the type of difficulties outlined in the Unlawful Conduct Report and discussed today, the Justice Department and law enforcement across this nation are committed to continuing to work together and with their counterparts in other countries to develop and implement investigative strategies to successfully track, apprehend, and prosecute individuals who conduct criminal activity on the Internet. In so doing, the same privacy standards that apply in the physical world remain effective online.

Mr. Chairman, the Department of Justice has taken a proactive leadership role in making cyberspace safer for all Americans. The cornerstone of our cybercrime prosecutor program is the

Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and became a Section in 1996. CCIPS has grown from five attorneys in 1996 to twenty today – and we need more to keep pace with the demand for their expertise. The attorneys in CCIPS work closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators," or CTC's, in U.S. Attorney's Offices around the nation. Each CTC receives special training and equipment and serves as the district's expert on computer crime cases. CCIPS and the CTC's work together in prosecuting cases, spearheading training for local, state and federal law enforcement, working with international counterparts to address difficult international challenges, and providing legal and technical instruction to assist in the protection of this nation's critical infrastructures. We are very proud of the work these people do and we will continue to work diligently to help stop criminals from victimizing people online.

I also note that public education is an important component of the Attorney General's strategy on combating computer crime. As she often notes, the same children who recognize that it is wrong to steal a neighbor's mail or shoplift do not seem to understand that it is equally wrong to steal a neighbor's e-mail or copy a proprietary software or music file without paying for it. To remedy this problem, the Department of Justice, together with the Information Technology Association of America (ITAA), has embarked upon a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. The "Cybercitizen Awareness Program" seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children an understanding of cyberspace

benefits and responsibilities, an awareness of consequences resulting from the misuse of the medium and an understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed.

Conclusion:

Mr. Chairman, I want to thank you again for this opportunity to testify today about our efforts to fight crime on the Internet while preserving the rights conferred by the Fourth Amendment and statute. Ultimately, the decision as to the appropriate parameters of law enforcement activity lies squarely within the Constitution and the elected representatives of the people, the Congress. The need to protect the privacy of the American people -- not just from the government but also from criminals -- is a paramount consideration, not just in the context of the Internet, but in general. The Department of Justice stands ready to work with this Subcommittee and others to achieve the proper balance between the important need for protecting privacy and the need to respond to the growing threat of crime in cyberspace.

Mr. Chairman, that concludes my prepared statement. I would be pleased to attempt to answer any questions that you may have at this time.

-original (since finished)

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the FBI's Internet and data interception capabilities and to help set the record straight regarding this important issue. I would like to first discuss FBI's legal authority for conducting interceptions on the Internet, and then describe Carnivore and how we use it.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search e-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting Carnivore as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly--and in fact this was the purpose behind the FBI choosing to share information regarding this capability with the industry experts several weeks ago. It is critically important that, as technology, and particularly communications technology, continues to evolve rapidly, the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. I believe that it is also very important that these discussions be placed into the context into which they properly belong and that the true facts concerning this issue are made clear. More to the point,

5/24/02 Release - Page 34

that these capabilities are used only with lawful authorization and that they are directed at the most egregious violations of national security and public safety.

First of all, the FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived in part from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), which is commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". I want to stress that all such interceptions, with the exception of a rarely used "emergency" authority or consent of a participant in the communication, are performed under a court order issued by a judge. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws must comply with the Fourth Amendment's dictates concerning reasonable searches and seizures, but they also include a number of provisions that are intended to ensure that this investigative technique is used judiciously and with deference to the privacy of intercepted subjects and certainly with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III and Department of Justice policy, applications for interception of oral, wire and electronic

communications require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can make an application to a federal court. Further, interception of communications is limited to certain federal criminal offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence-- not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are obtained. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently the court.

Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects and of others not named in the application.

To ensure privacy protection and evidentiary integrity of the communications that are intercepted, such intercepted communications are required to be recorded, if possible, on tape or other device, and recorded in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings are then required to be presented to the federal district court judge and sealed under his or her directions. The presence of the seal shall be a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extensions, the judge shall ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, providing notice of the order, the dates during which the interceptions were carried out, and whether or not the person was intercepted. Upon motion, the judge may also direct that portions of the contents of the intercepted communication be made available to for their inspection.

Any person who was a party to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the con-

tents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was intercepted in violation of Title III, ECPA or the Fourth Amendment.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may in a civil action recover from the person or entity engaged in the violation civil damages, including, if appropriate, punitive damages, as well as attorney's fees and other costs incurred.

The technical assistance of the service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This circumstance is increasingly the case with the advent of advanced communications services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders by specifying that a court order authorizing the interception of communications shall upon the request of the applicant, direct that a "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted."

In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are subject to the electronic surveillance laws like public officials and private persons. That is, unauthorized electronic surveillance is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in most cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices without lawful authorization from a court.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed orders, in order to be successfully implemented, require complex approaches to ensure that only messages for which there is

5/24/02 Release - Page 3

probable cause to intercept are, in fact, intercepted. The fact that court orders are becoming more detailed is in response, I think, to two facts.

First, the complexity of modern communications networks, like the Internet, as well as the complexity of modern users' communications demand better discrimination than for older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

The second fact is that for many Internet services, users share communications channels, addresses, etc. These facts make the interception of messages for which law enforcement has probable cause, to the exclusion of all others, very difficult. Court orders are therefore increasingly written to include detailed instructions for ensuring that the privacy of communications for which there is no probable cause to intercept is guaranteed.

In response to a critical need for tools to implement these complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs on a normal Personal Computer running the

Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion

5/24/02 Release - Page 41

that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected by a high impedance bridge and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that the Carnivore is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact raises the third issue--that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to

5/24/02 Release - Page 42

successfully implement, and comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using Carnivore is data integrity. As you know, Rule 901 of the Federal Rules of Evidence require the authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is also a key reason for the use of Carnivore over commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing, steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependant upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software.

5/24/02 Release - Page 43

I look forward to working with the subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank You.

5/24/02 Release - Page 44

Copyright 2000 eMediaMillWorks, Inc.
(f/k/a Federal Document Clearing House, Inc.)
FDCH Political Transcripts

View Related Topics

July 24, 2000, Monday

TYPE: COMMITTEE HEARING

LENGTH: 33615 words

HEADLINE: U.S. REPRESENTATIVE CHARLES CANADY (R-FL) HOLDS HEARING REGARDING THE **CARNIVORE** SYSTEM; WASHINGTON, D.C.

BODY:
HOUSE COMMITTEE ON THE JUDICIARY SUBCOMMITTEE ON THE

CONSTITUTION HOLDS HEARING REGARDING THE **CARNIVORE**

SYSTEM

JULY 24, 2000

SPEAKERS: U.S. REPRESENTATIVE CHARLES T. CANADY (R-FL), CHAIRMAN

U.S. REPRESENTATIVE HENRY J. HYDE (R-IL)

U.S. REPRESENTATIVE ASA HUTCHINSON (R-AR)

U.S. REPRESENTATIVE SPENCER BACHUS (R-AL)

U.S. REPRESENTATIVE BOB GOODLATTE (R-VA)

U.S. REPRESENTATIVE BOB BARR (R-GA)

U.S. REPRESENTATIVE WILLIAM L. JENKINS (R-TN)

U.S. REPRESENTATIVE LINDSEY GRAHAM (R-SC)

U.S. REPRESENTATIVE MELVIN L. WATT (D-NC)

RANKING MEMBER

U.S. REPRESENTATIVE MAXINE WATERS (D-CA)

U.S. REPRESENTATIVE BARNEY FRANK (D-MA)

U.S. REPRESENTATIVE JOHN CONYERS (D-MI)

U.S. REPRESENTATIVE JERROLD NADLER (D-NY)

KEVIN DIGREGORY, DEPUTY ASSOCIATE ATTORNEY GENERAL

Doc #14

DAVID GREEN, DEPUTY CHIEF

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

DEPARTMENT OF JUSTICE'

DONALD KERR, DIRECTOR

LAB DIVISION

FEDERAL BUREAU OF INVESTIGATION

LARRY PARKINSON, GENERAL COUNSEL

FEDERAL BUREAU OF INVESTIGATION

ALAN DAVIDSON, STAFF COUNSEL

CENTER FOR DEMOCRACY AND TECHNOLOGY

MATT BLAZE, RESEARCH SCIENTIST

AT&T LABS

BARRY STEINHARDT, ASSOCIATE DIRECTOR

AMERICAN CIVIL LIBERTIES UNION

ROBERT CORN-REVERE

HOGAN AND HARTSON

STEWART BAKER

STEPTOE AND JOHNSON

PETER SACHS

ICONN, LLC

TOM PERRINE, MANAGER OF SECURITY TECHNOLOGIES

SAN DIEGO SUPER COMPUTER CENTER

*** Elapsed Time 00:00, Eastern Time 13:04 ***

*

CANADY: The subcommittee will be in order. And it's probably going to be necessary for the staff to close the doors, otherwise we'll have noise from the hallways.

In recent years, with the growth of the Internet, the **FBI** has encountered an increasing number of criminal investigations in which criminal subjects have used the Internet to communicate with each other or their victims.

Because the **FBI** believes many Internet service providers lack the ability to discriminate between communications in order to isolate the specific types of information that may be authorized to be gathered under a court order, the **FBI** has designed and developed a program called **Carnivore** which enables the **FBI** to isolate, intercept and collect communications that are the subject of lawful orders.

The first news of **Carnivore** came in April during testimony before the Subcommittee on the Constitution by attorney Robert Corn-Revere, who represented an Internet service provider that tried to resist attaching the **Carnivore** program to its network.

It has also been reported that one of the nations largest Internet service providers, EarthLink, Inc., has refused to install **Carnivore** on its network because attaching the program in the past caused its remote access servers to crash, eliminating service to customers.

Other ISPs have stated publicly that they would challenge an order to attach to their networks.

While these industry officials have expressed willingness to cooperate with law enforcement to comply with legitimate court orders, they're concerned about the effects attaching **Carnivore** to their networks will have on the security of their infrastructure and the privacy of their customers.

At a press conference on July 12, Attorney General Reno stated that she does not want **Carnivore**, quote, "to be a tool that is in any way a cause of concern for privacy interests," close quote. Today's hearing provides federal law enforcement the opportunity to address the privacy concerns that have been raised.

More broadly, **Carnivore** raises the question as to whether existing statutes protecting citizens from unreasonable searches and seizures under the Fourth Amendment appropriately balance the concern of law enforcement and privacy. Law enforcement is concerned that the information needed to keep the public safe remains available. Individual citizens are concerned that a sufficient degree of privacy and the integrity of personal information be maintained in an age of modern communications and information storage where information that may have traditionally been kept in a file cabinet at home is now electronically stored by a third party in cyberspace. The hearing today will also address this balance of interests.

As we consider the use of **Carnivore**, it is important that our deliberations be based on facts and not on unsupported suspicions and irrational fears. At the same time, we should be sensitive to any potential for abuse of the **Carnivore** system. Even a system designed with the best of intentions -- to legally carry out essential law enforcement functions -- may be a cause for concern if its use is not properly monitored.

I look forward to hearing from all of our witnesses today and I'd now recognize Mr. Watt.

WATT: Thank you, Mr. Chairman.

I confess that up until about 10 days to two weeks ago, I had paid very little attention to this whole **Carnivore** project. And at about that point I started to get inquiring telephone calls from the media and press about what I knew about **Carnivore.** I don't know much more about it today, and that's why I want to start by praising the chair of the subcommittee for convening this hearing, because I agree with the chair that whatever information we have and however we proceed as a committee and as a Congress needs to be based on the facts.

So I try to bring to this hearing a level of open-mindedness to try to understand the facts and try to figure out with as much of an open mind as I can what disposition, if any, may be required by Congress, what legislative steps may be warranted.

I suppose I would be less than honest if I didn't say that I have had for quite a while a generalized concern about the government's ability to invade the privacy of its citizens. There seems to me to be a growing level of generalized concern about Big Brotherism that I suspect is being fed by the increasing electronic world.

WATT: When the Fourth Amendment was passed and put into the Constitution, there was at least a feeling that if the government came to do a search, it at least had to bring a warrant and present it to you or come and kick-in your door.

And in some of our communities, we have always had probably an exaggerated fear of whether the latter was likely to occur than the former, and it's probably from that perspective that I have always had this kind of generalized concern.

But notwithstanding that, I will make every effort I can to try to be objective and impartial about this issue. And I think those general comments point up the context in which we're operating and point up the importance of having such a hearing as this.

From my perspective it's good to see a number of people, who as long as the unwarranted searches and wiretaps and invasions or potential invasions were being visited on parts of the community that they weren't necessarily that interested in protecting any way -- it's great to see some greater exposure and concern being expressed about what our government does and how it does it. And this gives us an opportunity to look into that and evaluate it. And I welcome the opportunity and thank the chairman for convening the hearing for that purpose.

Thank you, Mr. Chairman. I yield back.

CANADY: Thank you, Mr. Watt.

Mr. Hyde?

HYDE: Thank you, Mr. Chairman.

Very briefly, this is a very important hearing, as attested to by the interest shown with so many people here today. But the tension between the law enforcement forces of our country, symbolized and personified by the **Federal Bureau of Investigation**, who need access to information if they are to stay on top of terrorists, counterfeiters, drug dealers, criminals of all sorts, the need for that information comes into tension with the need for the public -- for average citizens to have privacy, which is a very valued commodity. So that tension creates serious problems that it is the job of legislators to try to and solve. And that's what we're going to try and do in this hearing and succeeding hearings.

So I congratulate, you, Mr. Canady, for calling this hearing, and I welcome the statements of our friends, the witnesses from the **FBI** and others, and will follow this with great interest. Nothing could be more important in terms of national security and in protecting constitutional rights. I hope we get a good solution.

Thank you, Mr. Chairman.

CANADY: Thank you, Mr. Chairman.

Mr. Conyers?

CONYERS: Thank you very much.

Over the past few weeks, the details about this I hope misnamed technology has begun to emerge. We all know that it was only a matter of time before law enforcement would develop ability to conduct the equivalent of wiretaps on the Internet.

CONYERS: The news about **Carnivore** comes at a time when there is growing concern about how many Americans sacrifice their privacy by using it. Not only do web sites get all kinds of information about us when we make purchases online, or even when we just surf the web, but now we learn that the **FBI** can read our e-mails in the course of a criminal investigation.

So where I come from in the beginning on this is that, are we minimizing the interception of non-incriminating communications of a target of a wiretap order or are we maximizing the law enforcement access to the communication of non-targets? And I think this is a very important question that has to be resolved.

It's not at all clear that the law enforcement should use authority under pen-registers, to the pen-register statute, to access a variety of data. And it's not clear that law enforcement can install a super-trap to get the information that they think that they need.

Now, the Internet, as it takes its place along side the telephone and snail mail as a central means of communication, illegal activities are migrating there as well. And within constitutional boundaries, law enforcement tools -- law enforcement needs tools to be able to intercept unlawful communications by those who will use the Internet for illegal conduct in the hope that they can conspire without leaving fingerprints or footprints.

CONYERS: And at the same time, **Carnivore** -- I said I wasn't going to say that word -- at the same time, this system that we're looking at today mustn't bite off more than it can chew when it comes to **FBI's** electronic surveillance activities. Constitutional rights don't end where cyberspace begins.

And in many ways, today's hearing is not a new story. The potential for law enforcement to overstep constitutional boundaries for electronic surveillance on a new stage goes way back to the 1970s when the Church committee investigated the **FBI's** use of electronic surveillance against Dr. Martin Luther King Jr. The committee then recognized that technological developments in this century have rendered that most private conversations of Americans are vulnerable to interception and monitoring by government agents. So now in this new century, the Church committee's conclusion is timely -- is as timely as ever.

So should we now be comfortable with a "trust us, we're the government" approach? I don't think anybody on the committee has this view.

And I hope the hearing marks the beginnings of a careful examination of how the **FBI's** technology fits within the existing laws and the new technology. And I hope that this hearing will put to rest our fears about this system. Maybe they're unfounded. Maybe it's unclear and we'll need some legislative guidance for our law enforcement.

Does it give the **FBI** the ability to conduct indiscriminate searches of an individual's e-mail activity beyond what a court order would allow? Does it give the **FBI** the ability to search more than is permitted under the agency's pen-register and trap-and-trace authority? And why does the **FBI** need to put this system's terminals on-site at Internet service providers rather than letting the ISP turn over the information that the **FBI** needs, much in the same way the telephone company itself does.

These are the questions I'm looking forward to having some resolution -- and I'm happy that we're here inquiring into this matter.

I ask that the statement of another member, Congresswoman Zoe Lofgren, be included in these opening remarks.

CANADY: Without objection, it will be included in the record.

CONYERS: Thank you.

CANADY: The gentleman from Arkansas is now recognized for five minutes.

HUTCHINSON: Thank you, Mr. Chairman. And I, likewise, express my appreciation for your leadership on scheduling this hearing.

I want to just make a couple of brief comments. First of all, I want to extend my appreciation to the **FBI** and the Department of Justice for the way they have been open about this new technology.

HUTCHINSON: It's my understanding that you have allowed the media to review it; you have provided

demonstrations of this. And I think this is exactly the type of approach that we need to have when we're looking into a new arena of your legitimate needs for surveillance of suspects.

And I think the more the public knows, the more the Congress knows, and the more light that is shed, then the better judgments that will be rendered. And so, I do believe that the FBI has engaged in this Carnivore as a minimization tool, to limit the review of third- party documents as well -- or content -- as well as that of the suspect's.

But I think that there are some legitimate questions that need to be asked. One, is this new technique properly monitored? We're entering again into an arena that I did not have when I was a United States attorney back in the '80s. We had Title IIIs, we had court approval, we had pen registers, but this is a totally new environment. And I think that the FBI has to step gingerly, but we all, obviously, have a responsibility to engage in legitimate law enforcement activities in terms of surveillance.

But who monitors this? Another way to phrase the question is, who reviews and controls the appetite of Carnivore? I think that that is really what the purpose of this hearing is.

And as we go into the new arena of privacy, I think we all have to recognize how complex this is in its entirety. And for that reason, I want to finally mention, that there is a privacy commission bill that I've sponsored with Congressman Jim Moran of Virginia, a bipartisan bill that's moved out of the Government Reform Committee, should be coming up on the House floor. But this privacy commission legislation would set up a commission for the first time in 25 years to review our privacy laws. Whenever we had our last privacy commission, we didn't have the Internet. And yet they still called it privacy in the information age. And so I think it's time that we did review this again.

And one of the specific goals and responsibilities of the commission would be to review the activities of law enforcement in terms of privacy and its impact on privacy. So it's not just commercial, but it's also government, it is also law enforcement, a broad-ranging privacy commission. And this is one thing that we can look at not in a reactionary fashion, but in a steady, thoughtful fashion and set the tone as we enter into the next century.

So, with that, Mr. Chairman, I want to again thank you.

I look forward to the testimony of the witnesses.

CANADY: Thank you, Mr. Hutchinson.

The gentleman from Alabama is now recognized for five minutes.

BACHUS: I thank the chairman.

I think obviously what we have here is that technology has outrun the law. We have a Internet explosion, and I don't think the law has kept pace with it. I don't think the laws on the books fit very well with what we're talking about here today.

I have two concerns that I would express to you. One is that we have a balance between legitimate law

enforcement needs and the right of privacy, that we try to maintain that balance, which is a delicate balance.

The second is that we have a balance between our different types of communications. Because if we have certain types of communications where we have the potential to monitor everything that goes through them, but we have other types of communications that we're limited in our surveillance, criminals are going to be the first ones to figure out what is their safest mode of communications. And sooner or later you'll be -- if you have restrictions in one type of communications but not a lot of restrictions in another type of communications, the criminals are going to move to the least restricted or the least monitored form of communication.

And of course we've got to ask ourselves what level of monitoring do we as a country want to have on private conversations, to achieve what level of surveillance?

BACHUS: Let me give you an example. Today -- and this is an example, sort of, quote, "from the old world," but today, coming into this country, Federal Express packages are randomly opened, UPS packages are randomly opened, but U.S. mail is not. I mean, the mail is not opened. Now, criminals have pretty well figured out that the safest way of mailing something in the United States is not UPS or Fed Ex or parcel post, use the U.S. mail. The same going out. They've adjusted. They found out where the loopholes are. They found out where the least surveillance is, and they've gone with using the U.S. mail to send things, because they are not randomly checked.

The criminals are going to figure out, sooner or later, I would think -- and my question to you, aren't they going to figure out -- the illustrations you have given us is that you can take a work like "bomb" and you can search the Internet for bomb. Well, aren't our criminals -- aren't terrorists, for instance, aren't they very quickly going to realize not to use the word "bomb?" I mean, won't they figure out to use the word "dog" as opposed to "bomb"? As opposed to explosive device, won't they come up with some kind of other word? Won't they figure out a way, beyond you using key words, to get around this? And you're basically left on sweeping the conversations of law- abiding citizens? How do you get around criminals who are going to adapt to this system? They're going to be the first to adapt, to learn now to evade this system.

And at the same time my other concern is this: I've heard all sorts of assurances that this won't fall in the wrong hands, that there are safeguards. Well, today there are safeguards on **FBI** files. **FBI** files, only certain people have access to those files. Only certain people can have possession of those files. Only certain people can look in those files. Yet a few years ago, we found out that 1,000 of those files were over at the White House. What assurances do we have that we're not going to have another situation here where we have, like **FBI** files, that they got out of the restricted area and that people viewed them and perhaps utilized them for things they weren't intended to be?

You've read reports, I'm sure, that I have about IRS agents who pull people's income tax forms and they've used them to go up against their wives in court or their ex-wives on child support matters, or they've gone up against someone who was dating their girlfriend to try to embarrass them. And there've been all sorts of reports on what IRS agents did with files or what confidential information, which we were all assured would not fall -- would be restricted, where someone used those files within the IRS to their advantage or to embarrass someone else.

BACHUS: So I would simply say that, despite all the assurances, we know as a practical matter that there're examples, just recently, of restricted information being used for purposes which it was not intended.

So I'd ask you, how would this be any different? How is this any different from IRS information, which we were told would not be disclosed and has been in any number of cases? How is this any different from **FBI** files who found themselves being used for political purposes?

Thank you.

CANADY: Thank you.

We will now move to hearing testimony from our first panel. Our first panel will address the **Federal Bureau of Investigation's Carnivore** program and its role in federal law enforcement in the digital age.

On this panel first we would like to welcome Dr. Donald Kerr. Dr. Kerr is an assistant director of the **Federal Bureau of Investigation** and director of the **FBI's** Lab Division, which develops surveillance and tactical communications technologies.

Next we will hearing from Larry Parkinson, the general counsel for the **FBI.**

Following Mr. Parkinson will be Kevin V. DiGregory. Mr. DiGregory is deputy associate attorney general at the Department of Justice. Two members of the Justice Department's Computer Crimes unit -- Mr. DiGregory is joined at the table today by Christopher Painter, the deputy chief of the Computer Crime and Intellectual Property Section at the Department of Justice. Mr. Painter will not be making a separate statement, but will be at the table with Mr. DiGregory to answer questions.

I want to thank each of you for being with us here today and for patiently listening to our opening statements. I would ask that you do your best to summarize your testimony in five minutes or less, although I don't think anyone will insist on strict adherence to the five-minute rule. And without objection your full written statements will be made a part of the permanent record of today's hearing.

Dr. Kerr.

KERR: (OFF-MIKE) grateful for the opportunity to discuss with you our program for interception, lawful interception, of information on the Internet and data networks.

As you know, the use of computers and the Internet has grown rapidly and has been paralleled by the exploitation of computers, networks and databases to commit crimes and to harm the safety, security and privacy of others. Criminals use computers to send child pornography to each other using anonymous encrypted communications. Hackers break into financial service company systems and steal customers' home addresses and credit card numbers. Criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world. And terrorist bombers plan their strikes using the Internet.

Investigating and deterring such wrongdoing requires tools and techniques designed to work with new and evolving computer and network technologies. The systems employed must strike a reasonable balance between competing interests: the privacy interests of telecommunications users, the business interests of service providers, and the duty of government investigators to protect public safety.

I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception. In the interests of your time, I've submitted a longer statement, and what I'll do is try to summarize the high points, particularly addressing some of the questions the subcommittee's raised in opening remarks.

First, moving to how we protect the privacy interests of telecommunications users requires me to talk a little about the Carnivore system, what is it, how does it work. Put very simply, it's very much like what some in the networking industry would call a packet sniffer; that is, something able to pick out those packets using the addressing information of the Internet and only those packets to which we've been given access. It works by being placed at a service provider's location in order to get a part of the traffic that's passing through that service provider's portal.

In every case we require a court order. That court order is specific to the numbers we can target, if you will, the addresses we can target, and as to whether it's the equivalent of a pen-register, trap-and trace, or, in fact, full content recovery akin to a Title III intercept.

KERR: To be very clear on the point, we don't do broad searches or surveillance with this system. That's not authorized by a court order and, in my view, could not be.

The way it works, in detail, is that once the court order is issued, the system basically has a filter mask, and that filter mask is prepared with an understanding of the court order so that, for example, the Internet protocol addresses that are the legitimate target of the investigation are called out in the court order and set forth in this filter mask.

Second, we're able to also sort on the "to" and "from" line of the e-mail. And maybe the best way to think about that is think about the piece of standard mail. What it's basically allowing us to do is record the address to which the envelope is being sent and the return address on the outside of the envelope. We're not permitted to read the subject line, and, in fact, do not capture that and record it because we're not authorized to open the envelope with either a pen- register or a trap-and-trace order.

If we have an order that allows us to recover content, we're able to open the envelope. And in this case, what we would then do is capture all of the packets that relate to that e-mail in order to record them on a stable medium -- magnetic tape or some other stable medium -- for later reassembly at another location.

It's installed by a supervisory special agent who has training and experience in, in fact, responding to court orders of this sort, assisted by one of our electronic technicians, and, in every case, by one or more technical people from the Internet service provider.

And I think it's important for you to note that that team of people that records it, or puts the system in place, is not made up of the case agent leading the investigation. This is a technical team of three or more people. It probably also includes an electronics technician from whichever of our field offices is responsible.

We don't look at the text on site until it's recorded and returned, either to a field office or to us at headquarters.

And the installation, to put a picture in your mind, looks very much like a desktop personal computer. It's

often bolted into a rack like other equipment at the Internet service provider location, but an important difference is that it has no keyboard, no mouse, and, in fact, it's locked up, as far as the enclosure is concerned, where the magnetic media are written, because this, in fact, is the first step in the evidentiary chain. And so it's important that it be locked, access only provided to an agent who comes on site to collect the lawfully obtained information and treats it just like we treat physical evidence in terms of chain of custody from thereon.

An important further point is that we produce a record for audit of the filter-setting and the configuration on each installation. In the first few times that it was used, that was done by the people doing the installation. We've now grown concerned, because of discussions that have been ongoing, that we record that in a way so that it's authenticated, and so we now, in fact, override it with a hash, so that if someone tried to rewrite that audit trail, that could be detected.

And that record of filter settings and configuration, in fact, becomes part of the evidentiary record available to the court and the defense as required.

KERR: There are also sanctions for misuse, and no one should forget that. There are both criminal and civil sanctions that cover both Title III and Electronic Communications Privacy Act installations. It's a federal felony, calling for a prison term of up to five years, a fine, plus possible recovery of civil damages.

And so I don't think our technical teams installing these devices are going to risk their jobs, their integrity and their future by attempting to operate this equipment improperly at the ISP.

Moving on to the method by which we respect the business interests of the service providers: every installation has, in fact, been done in collaboration with the service provider's technical staff. To do it efficiently, we, in fact, only want to intercept the very smallest slice of the relevant traffic. And, in fact, where the ISP itself is technically capable of performing the intercept, that is, they have the equipment and the personnel, as many of the large ones do, so they can respond to the court order, we are, in fact, very happy for them to do that and simply provide us the information which is the subject of the court order and we never do install our equipment. We also, in those cases, bear some part of the cost of doing that.

ISPs come in all sizes. I think there are various numbers of them estimated in the United States at the present time, but it's upward of 10,000. They're not all large, listed companies. Some of them are more mom-and-pop operations. They don't have large amounts of equipment and a great deal of technical sophistication. And where the ISP cannot perform in a timely way under the court order, we are then willing to bear the technical and cost burden by installing our system.

Our system is passive on the network. It only receives information through the filter as authorized by the court order and it emanates no signals and no communications over the network. So we don't believe that it in any way would interfere with the proper functioning of the service provider's equipment delivering e-mail to customers.

And, lastly, the equipment is removed immediately upon the expiration of the court order. It does not remain at the Internet service provider, nor is there anyone who can get in and make a decision on their own to leave it in place.

Lastly, does it support us in carrying out investigations in our most important cases? We think it's a well-focused capability. It uses some of the very attributes of the Internet in particular the Internet protocol addressing capability, the "to" and "from" lines of the e-mail in order to restrict our collection to just those who are the targets of the court order. In a sense, it's automatic minimization up front.

Not to say there's not minimization after the fact, because when the messages are reassembled back at the field office or at headquarters, if we have, in fact, incorrectly or inadvertently captured information we shouldn't, it's, in fact, deleted at that time.

And it's really no different than the minimization that occurs first real-time on a Title III wiretap and then subsequent on the recording of that wiretap to be sure there's nothing there that shouldn't be.

It produces evidence with an appropriate first step in the chain of custody. We're trying to maximize the opportunity to properly gather evidence, authenticate it and be able to testify that we've neither added to nor subtracted nor altered that which we've captured.

It's a flexible tool, because it's a combination of software and hardware. And so we can, in fact, adjust it to fit subsequent court orders, and we can move from one case to another with it.

KERR: We maximize the use of commercial software to reduce risk and cost, and as I mentioned before, we've used authentication.

Finally, one of the things we're going to do, as a consequence of our discussion over the last 18 months, with people in industry, staff and members of Congress, five of the Department of Justice components, a number of U.S. attorneys, some 15 federal and state law enforcement agencies, we think it's important to lay to rest this question, Does this thing, in fact, do that which we say it does and only those things which we say it does?

And so we are working right now to undertake an independent verification and validation of the software that we use. We're going to do it with academic members of the team as well as industry members. And by the way, we're not going to contract for those people; they'll be selected by the organization that carries this out for us.

But what we're going to do, is very akin to what, for example, NASA does with software developed for their launch operations: ask some independent party to verify that the software that we have and deploy will, in fact, do those things that we say it will and not provide capabilities that we should not have.

Our year-to-date use of this tool, that is this present year -- the first three quarters of the fiscal year, we've deployed it some 16 times. It's been used six criminal cases and 10 national security cases. Some number of those were simply pen-registers, some involved full content. None of those cases have been adjudicated, so we can't speak to details today, but I think it's probably of interest that it's not a very large number. It is reported in the annual wiretap report in that category called "other," so if you're wondering where the number will found, either now or in the future, that's were it will be.

In summary, I think we've tried to develop a tool, not in advance of policy and precedent, but, in fact, with a great deal of care in understanding the legal authorities under which we are authorized to use this and to target it precisely and well at those that the court orders.

Thank you very much, Mr. Chairman.

CANADY: Thank you very much.

Mr. Parkinson?

PARKINSON: Thank you, Mr. Chairman. I do not have a prepared statement. I'll be very brief.

I want to echo, first of all, what Dr. Kerr said, and this is -- despite its unfortunate name, this is a tool that is very surgical. And I think Representative Hutchison had it right, that this really is a minimization tool. And I'll leave the technical aspects to Dr. Kerr.

What I'm here, primarily, to emphasize -- and I'm delighted to be here and answer any questions that the committee may have -- is to emphasize that there -- the FBI and the Department of Justice have a true commitment to the rule of law. And I want to respond just briefly to the notion that we have deployed this system without controls or without proper authorization. That is simply not the case.

PARKINSON: We are also not saying, Simply trust us, we're the government. I think we have -- we're not naive. We have -- we've had enough situations in the course of our history to know that that's not enough. We have significant oversight, both within the bureau, within the Department of Justice, and most importantly, within the judicial branch that overseas deployment of this device and any other surveillance device.

In addition to that, we obviously have vigorous and appropriate congressional oversight.

So that's why I'm here. I'm happy to answer questions. And I just want to emphasize to you and to the American people that this is a tool that is deployed rarely and it is never deployed without a court order. And we do not deploy it in a way that exceeds the court order.

It is very discriminating, and I hope that this gives us the opportunity to explore that and give some comfort to the committee as well as to the American people.

Thank you very much, Mr. Chairman.

CANADY: Thank you, Mr. Parkinson.

Mr. DiGregory?

DIGREGORY: Thank you, Mr. Chairman.

Mr. Chairman and members of the subcommittee, thank you again for allowing me this opportunity to testify about the law enforcement tool, **Carnivore**, and the Fourth Amendment.

We have seen, as Dr. Kerr has noted, magnificent growth of the Internet over the last 10 years, and it has created vast benefits for our citizens, our businesses and for governments, and it seems to hold boundless promise if we can harness it.

The Internet has spurred a new and thriving economy. Many businesses have prospered by providing their products and services through the Internet. Others have assisted in the building, maintaining and improving the Internet itself. The Internet has given people jobs, supported families and communities, and created new opportunities for commerce for America and for the world. The Internet has touched both our working lives and our family lives.

As we have seen throughout history, however, there are those who would use powerful tools of progress to inflict harm upon others. The Internet has not escaped, unfortunately, this historical truth. Even in the Internet's relatively short existence, we have seen a wide range of criminal use of this technology. It has been used to commit traditional crimes against an ever-widening number of victims.

There are also those criminals intent on attacking and disrupting computers, computer networks and the Internet itself.

In short, although the Internet provides unparalleled opportunities for Americans to freely express ideas, it also provides a very effective means for ill-motivated persons to breach the privacy and security of others.

Many of the crimes that we confront every day in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft and child pornography are migrating to the Internet.

The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails property to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution.

If law enforcement is too timid in responding to cyber-crime, however, we will in effect render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime without fear of authorized government surveillance.

If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought about by the information age.

Proper balance, Mr. Chairman, is the key.

Now, despite the fervor over **Carnivore,** the truth of the matter is that **Carnivore** is, in reality, a tool that helps us achieve this balance.

To satisfy our obligations to the public to enforce the laws and preserve public safety, we use the same sorts of investigative techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional and legal limits that are imposed upon us.

Carnivore is simply an investigative tool that helps us to investigate online in the same way as in the physical world and enables us to obtain only the information we are authorized to obtain through a court order.

To illustrate: Law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products or to whom the drug dealer is selling his goods. It is therefore important to determine with whom the drug dealer is communicating.

In the olden days of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through the use of telephones and pagers.

DIGREGORY: Law enforcement would obtain an order from a court authorizing the installation of a trap and trace and a pen-register device on the drug dealer's phone or pager.

Now that same drug dealer or kidnapper or a child pornographer may be just as likely to send an e-mail as to call his confederates in today's world.

When law enforcement uses a trap and trace or a pen-register in the online context, however, we have found that at times, the Internet service provider has been unable or even unwilling to supply this information. It is for that narrow set of circumstances that the **FBI** designed **Carnivore.** Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like **Carnivore.**

Carnivore is, in essence, a special filtering tool that can gather the information authorized by a court order and only that information. It permits law enforcement, for example, to gather, pursuant to an order, only the e-mail addresses of those persons with whom the drug dealer is communicating without allowing any human being, either from law enforcement or the service provider, to view private information outside the scope of the court order.

In other words, as I understand it, **Carnivore** is a minimization tool that permits law enforcement to comply with court orders, to protect privacy and to enforce the law to protect the public interest.

In addition, as Dr. Kerr has noted, **Carnivore** creates an audit trail that demonstrates exactly what it is capturing.

And as with many other investigative tools, there are many mechanisms we have in place to prevent possible misuse of **Carnivore.** The Fourth Amendment and the courts, of course, restrict what law enforcement can do online with or without **Carnivore,** as do the statutory requirements of Title III and the Electronic Communication Privacy Act.

In the case of federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example, before **Carnivore** may be used to intercept wire or electronic communications, with a limited exception of digital display pagers, the requesting investigative agency must obtain approval for the Title III

application from the Department of Justice.

Specifically, in the Department of Justice, the Office of Enforcement Operations in the Criminal Division reviews each proposed Title III wiretap application for content to ensure that that interception of content satisfies the Fourth Amendment requirements and is in compliance with applicable statutes and regulations. If the proposal clears the Office of Enforcement Operation, approval must generally be given by a deputy assistant attorney general in the Criminal Division. Typically, investigative agencies such as the FBI have similar but separate internal requirements. If the investigative agency and the Department of Justice approve a Title III request, it still must, of course, be approved by the proper court using familiar but exacting standards.

By statute and internal regulation, the interception may last no longer than 30 days without an extension by the court, and courts also often impose their own additional requirements. In addition, remedies for violating Title III or the Electronic Communication Privacy Act by improperly intercepting electronic communications include criminal and civil sanctions. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Despite this panoply of protections, we recognize that concerns remain about this tool. And as Dr. Kerr has noted, the attorney general has asked for an independent review of the Carnivore source code to ensure that its capabilities are what we understand them to be. A report generated from the review will be publicly disseminated to interested groups within industry, academia and elsewhere and should alleviate any concerns regarding unjustified intrusions on privacy from the use of this tool.

Mr. Chairman, my testimony today necessarily highlights a few of the more significant aspects of the balance between privacy and security that the department believes must be struck.

DIGREGORY: The Department of Justice has provided the committee with my full written statement, and it is my sincere hope and expectation that through this and other fora those of us who are concerned about privacy and public safety will recognize that responsible law enforcement can enhance both goals.

Mr. Painter and I are available to try to answer any of your questions along with the rest of the panel.

Thank you, Mr. Chairman.

CANADY: Thank you very much.

Let me say to each of you who have testified that I think your remarks have helped clear up at least some of the questions that have been raised about the system called Carnivore, and I think your testimony has been very helpful to us.

I'm going to have a few questions and other members will have questions. I do want, at the outset, to acknowledge that we probably not get to all the questions that we want to ask, so we would ask you to provide us written responses to any additional questions that any members of the committee may have, but also give you an opportunity to provide any additional comments that you wish to make in light of subsequent testimony that comes in the hearing today.

Let me -- having said that, let me go over some ground that I think you've already covered concerning the use of **Carnivore** under the pen- register or trap-and-trace authority.

When you're using the pen-register or trap-and-trace authority, would you ever obtain any letters or information other than those that make up an e-mail address, such as JohnSmith@home.com? In other words, have you ever or would you ever make a request, under the pen- register or trap-and-trace authority, that included the capture of words or sentences other than the e-mail address?

KERR: The answer from our side in terms of how we set it up is that if it's a pen-register order we only get the two address and we capture nothing else.

PAINTER: And I might say also that the -- even the subject line we consider to be content, and that would require a full Title III. It's just the addressing information and that solely, just as in the telephone context, the numbers dialed, the numbers received.

CANADY: OK. So it's your understanding that your legal authority is limited to the e-mail address, and, of course, it has been your practice -- it is your practice and has been your practice only to obtain the e-mail address when you're using the trap-and-trace or the pen-register authority.

PAINTER: In the electronic communications context, yes, that's correct.

CANADY: Let me ask you this: In your view, does federal law enforcement have the authority under the Pen Register Act to capture so-called URL addresses, which are the addresses of the web sites a person has visited?

PAINTER: If the URL address -- the URL addresses are not really what's contemplated under the pen-register, trap-and-trace statute. What we're talking about there is -- I mean, it could -- it's possible it could be captured if it, for instance, was a Hotmail service. A Hotmail service, as Dr. Kerr can talk about more specifically in a technical way, is a web-based e-mail service, and so you would capture that part of it that identifies is it a Hotmail service and then specifically limits it to a specific authenticating code. And I think Dr. Kerr can talk a little bit about that.

CANADY: If you would.

KERR: Yes, I think that's a very good point. There are services, such as Hotmail, where we have to capture the web page and then look for the authenticators and other indications that it's an e- mail service. Having done that, we limit the collection to simply the e-mail that's provided through that service. We don't capture the users other use of the Internet, we are not interested in what they do when they surf the web, and we restrict what we do only to that e-mail traffic over the web page.

CANADY: OK.

Now, in your comments, Dr. Kerr, you indicated that **Carnivore** has been used only a few times. I think 16 was the number for this year, is that correct?

KERR: That's correct; 16 times this year. I think about a total of 25 in the life of the program over the last

two years.

CANADY: Well, over that same time period, how many Title III intercepts on e-mail would you have done not using **Carnivore**?

KERR: We've used **Carnivore** and earlier versions of the same technology, and in some other cases, we've used a commercial product to try to capture e-mails. And one reason that we moved from the commercial product to **Carnivore**, was, in fact, to get some of the selectivity and audit properties that I briefed you on earlier, because the commercial product had been developed for quite another purpose.

Products like this are used by the service providers to monitor the quality of their service. In that case, they have no legal restrictions on what they can observe. In our case, we're quite limited and need the more discriminating technique.

CANADY: My time has expired, but by unanimous consent, I'll have three additional minutes.

Let me follow up on that, if -- let me change, given the limited amount of time, to a different subject.

How many -- have you contemplated allowing the use of **Carnivore** by other, not only federal law enforcement agencies, but state or local law enforcement agencies?

KERR: At this point in time we have used it on at least one occasion in support of another federal law enforcement agency. We have not yet brought it to the point where we would be talking about it in terms of providing it to state agencies.

As you're aware, the authorities under which they operate are different than at the federal level. And so, we're not necessarily assured at this point in time that it would be a suitable tool for us to turn over.

That said, anytime we turn over Title III or other intercept equipment to state and local authorities, we do so with the signature of the attorney general. She has, in fact, the decision on that; we don't.

CANADY: In my opening statement, I made reference to a media report that Earthlink was required to attach **Carnivore** to its network, in one instance. And doing so, caused part of its network to crash and its customers to lose service.

Now, from your comments, Dr. Kerr, I understand that that just shouldn't happen. I'd like to hear your comments about those reports and what actually took place there and whether this system can pose a threat to the functioning of an ISP, and whether you've had other complaints similar to that made by Earthlink.

KERR: In the specific case, what I will do is try to give you something for the record that's more complete than I can do right now. But initially when we went to Earthlink and they were ultimately compelled to move ahead to do this, they attempted to do it themselves with software that they essentially tried to put together in real time.

KERR: It didn't work and it didn't provide information consistent with the court order.

It's not clear to us that anything we subsequently did had any averse affect on their network. And, in fact, in at least one other case, we've had quite good cooperation from them.

It's the only case where we've, in fact, had to go back and get the judge to emphasize that he meant the order. In all other cases, we've had excellent cooperation, particularly at the technical level and normally at the level of the general counsel of the company involved.

PAINTER: I would add also that in any of these cases, you have to work with the service provider to actually install this. The FBI couldn't go in and just do it themselves. So even when the court orders it, and that happens in each case, you have to work with the technical people to install it.

CANADY: Thank you very much.

Mr. Watt's recognized for five minutes.

WATT: Thank you, Mr. Chairman.

Let me start at a pretty basic level, Dr. Kerr, and pick up on something that you said in response to one of Mr. Canady's questions, having to do with your sharing of this tool with other law enforcement agencies.

And as I recall, your response was that the authorities of the states are different than the authority under which you are operating.

Unless I'm missing something, everybody's operating under the Fourth Amendment to the United States Constitution, so unless you are saying that the Wiretapping Protection Act gives the federal government some additional authority then the states are able to exercise under the Fourth Amendment to the Constitution -- well, maybe I shouldn't speculate about what you are saying.

Tell me what it is you are saying when you say that you are operating under a different authority than the states.

KERR: I would certainly take your point that the states are operating under the same Constitution that we are. But we, in addition, of course, have the Title XVIII statute that guide the federal use of electronic intercept.

WATT: But that's in -- I would take it that that is in furtherance of whatever authority you have as a basic proposition under the Constitution of the United States. It doesn't give you any additional authority, does it?

KERR: No, it certainly doesn't. But the point is that some states, in fact, do not have a statutory basis for state and local law enforcement to do electronic surveillance or they have statutory limitations, all still within the Constitution but, in fact, more restricted or nonexistent in some cases.

WATT: All right. Let me ask another pretty basic question: How long has **Carnivore** or some predecessor form of **Carnivore** been in use by your department?

KERR: Roughly two years. The program began, in terms of a development program about three years ago, but in terms of actual court orders and deployment, over the last two years.

WATT: Square for me, if you would, the notion that you have now engaged in 25 uses of this, 16 of them this year -- or are engaging in them, I guess, on an ongoing basis, because none of them have come to trial yet, and the statement that you made that you are now undertaking or preparing to undertake verification that this system does what you say it does and that only.

WATT: It seems to me that such verification would have taken place at some earlier stage, not 25 cases into public concern or legal concern.

KERR: The essence of the development program, of course, is that you do learn as you develop and deploy. We, as I pointed out, had initially tried to use a commercial product and found that it did not have all of the properties we thought should be in place for long-term use in a law enforcement context. And so we...

WATT: What products -- what properties did it not have that you were looking for?

KERR: It didn't have the same discrimination capabilities. It didn't have the same ability to provide an audit report and report on configuration that we require.

WATT: Now, who is it that -- now that you have the audit capability -- who is that has the oversight in your department to audit what -- to really review the information that you obtain from the audit?

KERR: I think that'll actually happen quite outside of the **FBI** in that the results of the intercept will, in fact, be provided to the court. They will, of necessity, become available to the defense. And consequently, they will be more aggressively questioned, in fact, in that circumstance than they would be in any internal administrative review.

CANADY: The gentleman's time has expired. The gentleman will have three additional minutes.

WATT: Let me turn to a different area if I can. You've compared this to -- the Internet capabilities this -- analogous to a phone tap or the authority that you have to tap phones.

Does your authority to tap phones get you into the internal phone mechanisms of the phone company or is your authority limited to tapping individual phones of individual suspects?

KERR: That's an area that's, in fact, in a state of change today.

WATT: Who's changing it?

KERR: You did, sir...

(LAUGHTER)

... in that the...

WATT: I think I've -- you being Congress, I take it?

KERR: Yes, sir.

WATT: I think I voted against this bill, as I recall, and still have some concerns about it, to be honest with you.

But go ahead, I'm locked with everybody else for that purpose.

KERR: Sorry.

Some of my colleagues know this better than I, but the point is, the Communications...

WATT: Maybe I should be directing this to Mr. Parkinson. He's the general counsel. He should know these things, I guess.

Or Mr. DiGregory. I didn't mean to beat up on the technician here. I'm just...

DIGREGORY: In its most basis sense, as I understand it, the telephone tap is conducted at the phone company but is restricted to the individual line which you wish to tap. Whether you wish to obtain numbers dialed, numbers coming in, or whether you wish to obtain content.

WATT: OK. Now how do you -- how does that compare with the capability that **Carnivore** has for Internet communications?

DIGREGORY: Now, we'll go back to the science side.

KERR: Not to try to confuse you by switching back and forth, but the telephone...

(CROSSTALK)

WATT: I'm pretty confused without you switching back and forth, but go ahead.

KERR: The telephone tap refers to the ability to intercept switch circuits, which was the basis historically of the telephone system. The Internet provides a different kind of technology that we're trying to intercept. It's a so-called packet-switched network. And it doesn't work by my, in effect, leasing a circuit in order to make a phone call from my house to yours, and that's, if you will, for the time of the conversation, our private circuit.

WATT: Let me stop you right there, because my light's going to go off -- has already gone on.

If you needed additional legal authority to get mobile home phone taps, why would not additional legal authority be necessary to -- for you to be doing what you're doing under this system? And maybe again...

(CROSSTALK)

KERR: I'll give you my view and then...

(CROSSTALK)

CANADY: The gentleman has an additional minute.

KERR: ... I'll stand corrected by my colleague.

We do, in fact, have legal authority to do what we're doing today. And I think it's because of the correct belief, from my perspective, that the addressing information on the Internet is, in fact, a useful and appropriate analog to the telephone number in the switch circuit world.

But perhaps, Mr. Digregory or Mr. Parkinson would like to add to that.

PARKINSON: I think that's correct and it's appropriate also to point out that there are gradations of authority, and there's a higher level of authority within the department and a higher level of authority in the courts, depending on what sort of intrusion you're talking about. If you're talking about simply numbers, then we have the pen-register trap-and-trace authority; if you need to go beyond that then we have to move it up a notch or several notches to a Title III authority.

WATT: Thank you, Mr. Chairman.

CANADY: Chairman Hyde?

HYDE: Thank you, Mr. Chairman.

You can understand the skittishness of some people whose concern is privacy. And when you see some of the things that have happened here in Washington, it gives one reason to wonder and to worry.

I speak of the Defense Department releasing an employment application with information that was supposed to be private and it ends up in The New Yorker magazine. And that person -- I think he got a letter, mildly critical of what he did, which doesn't go in his file and no prosecution.

A less compelling case, I case, is over the so-called Filegate where the law wasn't breached at all, but one's sense of privacy was -- took a beating, I should think. And so, there are people who are skeptical about how this culture of privacy -- how porous it is. That doesn't call for an answer, that's just, kind of, a comment.

HYDE: Can you tell us how -- I'll ask this maybe of Mr. DiGregory -- how terrorist cells and organized crime and others use technology and how does **Carnivore** address the growing use of technology by criminals?

DIGREGORY: Well, I think that terrorist cells and organized crime can use the Internet to communicate, can use e-mail to communicate. And simply the same way that a pen register addressed their use of the telephone to perpetrate their criminal activity, **Carnivore** addresses -- or can address their use of the Internet with respect to those activities and obtain, pursuant to a pen-register order, those numbers that are being called by the organized crime figure or the drug trafficker.

HYDE: Could you tell me what reasons you have for not letting the Internet service providers gather the requested information? I take it they have made themselves available to do that for the most part. Maybe some of them haven't. But what are the reasons why you don't let them do it?

DIGREGORY: I don't think it's a question -- and anybody up here is invited to correct me if I'm wrong -- I don't think it's a question of not letting them do it, I think **Carnivore's** use is limited to those situations where the Internet service provider is unable to provide the minimized court-ordered information that the **FBI** requires, pursuant to the order.

KERR: And let me amplify on that a little bit.

The **FBI,** my understanding is, will always allow the Internet service provider to do it if they can, in fact, do it in a timely fashion.

The one time this was actually challenged -- now talking about who the ISP was -- and that one instance the ISP tried to work with their own tool, it was not effective, it was not capturing all of the addresses. It was only capturing incoming and not outgoing addresses. It wasn't giving the whole information. And in that case, the **FBI** was forced to use the **Carnivore** tool.

That is not their first line. The first line is to let the Internet service provider do it if they can. And, in fact, the **FBI** I believe would like the Internet service providers to do it if they can.

HYDE: Fine. Thank you very much. I have no more questions.

I'm through, Mr. Chairman.

CANADY: The gentleman from Michigan's recognized.

CONYERS: Thank you very much.

I think one of the basic questions here is to determine whether or not you're minimizing your activities or whether you're maximizing them. And of course, it's already been asserted that you're minimizing them. And my job is to find out, maybe before the hearing ends but certainly after the hearing, whether that is correct.

And it seems to me that this system that we're oversighting today, unlike other trap-and-trace devices, or the others that we use, is available for -- is subject to the maximization of information, getting more information than is required or is authorized by a court order. And so that's the area that, to me, is very, very unclear as of now.

I'm not sure how we're going to sort this out, but I think we have witnesses here that are going to come forward later on that are going to complain about the fact that there was other information that was available through this system that might not have been available if we weren't going through the Internet.

CONYERS: Isn't that possible, that you can get more information, you can look at other things that would not have otherwise been available?

KERR: One of the points, Mr. Conyers, that I was taking some time with was to try to make it clear that the only information we can capture is, in fact, that specified in the court order. And to go outside of the court order, in fact, is a federal felony with substantial sanctions for those who would do so.

We, in fact, think of this as a tool that's designed explicitly to meet the requirement of the court order. We don't have the authority, nor are our people allowed the opportunity, to step outside of those bounds.

CONYERS: Well, right, that's the law. But, I mean, that's the problem. I mean, if I could be assured that everybody wouldn't do the wrong thing because there was a statute making it criminal, that would reduce a lot of our efforts. And even law enforcement people, I hasten to add.

Mr. DiGregory?

DIGREGORY: Mr. Conyers, as I understand the way the system operates -- and certainly, that's correct, that's what the law is. But there are checks and balances with respect to **Carnivore** which would make it extremely difficult for someone to counter those checks and balances and violate the court order.

It's not just a situation where, as I understand it, a rogue **FBI** agent, for example, could broaden the coverage of the **Carnivore** intercept and violate the court order. In order to do that, he would need to engage the aid of technical people, perhaps even technical people at the Internet service provider, and he would also have to find some way to cover up or change the audit trail that is left by the system so that it doesn't expose his going beyond the court order.

And, again, I'll stand corrected by those who are more expert in the way this system functions, but that's how I understand it. And although, yes, that's the law, there are checks and balances which would make it

extremely difficult for someone to violate the court order.

KERR: And it's also a law we take very seriously. If a law enforcement person violates the wiretap law, they'll be prosecuted. The Computer Crimes Section has a responsibility for doing that and would prosecute particularly law enforcement individuals who violate the wiretap law.

DIGREGORY: And we've done that. Not in the context of these kinds of intercepts, but in the context of telephone interceptions.

CONYERS: So our assurances are that, first of all, there's a law against it which you would assiduously prosecute your own people were they to violate it, and that there are other technological measures that make it very difficult to do anyway. There's a box that actually can search to preclude getting more information than you want. Is that the way I understand that it operates, Dr. Kerr?

KERR: Actually, the way it works is that it's set up in conformance with the order to collect and record that which is part of the order. And in doing that setup and arranging the configuration, the knowledge of that setup and configuration is, in fact, recorded right along with the evidence. Once that evidence is collected, it's, in fact, delivered to the federal court where it's sealed by the judge who issued the order and with an appropriate chain of custody to get it there.

CANADY: The gentleman's time has expired. Without objection, the gentleman will have three additional minutes.

CONYERS: Thank you. I'm not sure if I need them, Mr. Chairman, but let me just say that -- I don't know, maybe the committee is put in a more difficult position than I appreciate.

CONYERS: I don't know if we have any way of verifying that the technological part of the response to my question that you've given me, and I know that, you know, unfortunately in the past, we've had many agencies, including law enforcement, that have gone beyond the scope of their responsibility. There's hardly anything new about that.

So I'm trying to figure out how we're going to get to the bottom of this. We made need a -- we may need technology experts to match yours to verify that what you're telling us makes everybody believe that it's OK, it's the government. And that's what I'm not sure.

GRAHAM: Will the gentleman yield?

CONYERS: Of course.

GRAHAM: I think the gentleman raises a valid point, but I think that that has already been addressed, to a certain extent, by the department's announced plan to have this system reviewed by an independent body of experts who would issue a report that everyone could examine. And I suppose, ultimately, representatives of the independent body of experts could come here to the Congress and answer questions that we might have of them, based on their independent review.

CANADY: Would the gentleman yield from questioning?

CONYERS: Well, yes.

CANADY: Thank you, I'm just concerned about that. Let's assume that an independent body of experts reviewed this system and said it was fine and would do only what it was suppose to do, et cetera, that could change at any time after that. And how would you maintain the trustworthiness that the system was still limited after they had investigated, unless you were going to have an independent group looking over the **FBI's** shoulder forever? Because obviously you can't trust the police agency forever not to go beyond what they're supposed to do.

CONYERS: Well, I raise this, Chairman Canady, merely to point out that we're, sort of, in the process of taking words for it. And, of course, we're happy to take the government's words, but, you know, this -- as I recall it, **Carnivore** didn't -- wasn't sent to us, we, sort of, found out about it in the scope of things, and it began to take on a life of its own that led to this hearing.

So I'm anxious to hear from the non-government witnesses to see how their understanding of what has been happening and -- with this system comports with what we're being told. But I thank the witnesses, anyway; that's what your job is about, that's what you're supposed to do.

Thank you, Mr. Chairman.

CANADY: Thank you, Mr. Conyers.

The gentleman from Arkansas, Mr. Hutchinson, is now recognized for five minutes.

HUTCHINSON: Thank you, Mr. Chairman.

On that particular point, you all are willing to submit the source codes to an independent review and audit. I think the dispute is that the ISP community would like to have open access to the source codes for purposes of reviewing it and determining it's authenticity and that it accomplishes what you desire.

What problems would you see, if any, in allowing open access to the source code that make up **Carnivore**, Dr. Kerr?

KERR: There're two points that we would raise. We wouldn't have any problem releasing it to a group set up to do verification and validation. We would have a problem with full open disclosure, because that, in fact, would allow anyone who chose to develop techniques to spoof what we do an easy opportunity to figure out how to do that.

Beyond that, some of the code we have used is, in fact, commercial off-the-shelf software, and its proprietary to the companies that have developed it, and we're not at liberty to divulge their source code under the license that we've paid for.

HUTCHINSON: So you would be open, though, and it would not compromise legitimate law

enforcement activities, if there was a ongoing review system of the source codes for **Carnivore** or any subsequent adjustments to it.

KERR: I think the only concern we'd have at some point is, you know, when is enough enough? Do you review it each time you set it up for a new case? I don't think that's workable. Do you do it as part of an annual review of electronic surveillance beyond simply counting the occasions when it's in use? That may be more workable.

But clearly, when the number of reviewers are larger than our group that develops the system, we probably have reached some form of imbalance at that point.

HUTCHINSON: Thank you.

Now, let me -- if you have a content court order to use the **Carnivore** system, then, of course, you have to show probable cause, you've got to get your court order. But at that point, is innocent third-party information reviewed by **Carnivore**?

KERR: If we have, in fact, gotten proper information on the target addresses and the "to-from" -- because that's important, too, since more than one person might be using a particular computer -- in principle, we should only get the authorized communication.

That said, if we were to find that we had, in error or because of misinformation, recorded something to which we were authorized no access, we would have to minimize that just as we would on a normal telephone wiretap.

HUTCHINSON: It's been explained to me as a pipe in which **Carnivore** looks at all the data going through the type to seize that which is the subject of the court order.

KERR: Right. In fact, one of the...

HUTCHINSON: Is that pretty much...

KERR: Yes, one of our...

HUTCHINSON: The question...

KERR: ... problems is that the pipes are too big for us to do that and we rely on the service providers to give us just part of the traffic coming through their big pipe.

HUTCHINSON: And I've learned on computers that sometimes delete does not mean delete, that information continues to be stored. And so my question is: Is the information that is not captured pursuant to the court order, is it ever retrievable in any form by any means?

KERR: No, it's not, because it's all in random access memory and volatile memory. So, for example, if the

power goes off, we will lose everything in that memory. None of it gets to the...

HUTCHINSON: What if the power doesn't go off?

KERR: Well, none of it gets to a stable recording medium like magnetic media in a hard drive or a ZIP drive, a floppy disk. Only that which we're authorized and which the filter is set up for gets to that permanent media.

HUTCHINSON: Now, you indicated that year to date **Carnivore's** been used 16 times, I believe 20 times in all total. How many of these -- of course, these are the ones that's used the **Carnivore**, is that correct? But you also, in addition to that, use court-ordered wiretaps or pen registers to retrieve Internet information by using ISP capabilities.

KERR: In some of the cases, we've, in fact, been able to ask the ISP and they have provided us the information.

HUTCHINSON: I'm trying to get a contrast. The 16 that you mentioned, were these not by using ISP capabilities? This is when the **FBI** went in and used the **Carnivore** system; is that correct?

KERR: That's correct.

HUTCHINSON: All right. So I'm trying to get an idea how many others are out there that were used by ISP capabilities.

KERR: I don't have the number with me. We could certainly provide that to you.

HUTCHINSON: Does anyone know that? I mean, I'm trying to figure out if we're looking at 100 others versus 16.

PAINTER: My understanding for the Title III intercepts is that it is not a large number. Trap-and-trace, it might be a little larger. We can try to obtain those...

(CROSSTALK)

PAINTER: ... Dr. Kerr's indicated -- provide it to the committee.

CANADY: The gentleman's time's expired. The gentleman will have three additional minutes.

HUTCHINSON: Thank you.

I mean, it just strikes me that -- I mean, considering the number of Title III wiretaps of telephone communications, I mean, that's much greater than the 16 or what you've used by ISP. And I guess what I'm leading to is that it looks like, if the bad guys are moving as the whole population is moving to data communications through the Internet, looks like we're missing a whole lot here, that we're really only on

the surface of what we might need to be doing.

KERR: That's certainly true. The tool we've been discussing to this point today, **Carnivore** has, in fact, only been used in the framework of e-mail intercept.

KERR: As you're properly pointing out, there's a lot of other traffic on the network. We continue to work to try to see how we could develop appropriate and lawful tools to go after that traffic as well.

It would tend again to try to use the properties of the network itself; the need for me to be able to move data from my computer to your computer and capture it because of the addressing information that would be there, not by trying to view the content on the fly.

GRAHAM: Would the gentleman yield?

HUTCHINSON: Yes, I'd be happy to yield.

GRAHAM: I don't understand what other kind of traffic you're talking about if it's not e-mail. What realm are we talking about if we're not talking about e-mail?

KERR: Well, one could use other protocols, for example, to move large files, to move imagery, to move larger quantities of data. And it wouldn't move as e-mail in the sense that we've been talking about it today with a, you know, "from me, to you, subject," whatever. It might just move as a block of data. It could, in fact, be information that companies are moving from one location to another.

HUTCHINSON: Have you ever had an occasion to try to retrieve any of that information pursuant to court order?

KERR: We have not had any occasion that I'm aware of where we've tried to intercept that kind of information. In general, large files like that, we would expect to come to rest someplace and we would probably be picking it up as another part of an investigation.

HUTCHINSON: Finally, there's -- looking ahead a little bit, there was a question asked of whether the pen-register orders that are applied to the Internet reveal far more than the numbers that are dialed in traditional telephone wiretaps. And I know that you're restricting it to "to, from" information. You've specifically deleted capturing the subject information because that would be content- oriented.

But this is still a concern. I guess that even the "to" with the address, sometimes a descriptive term -- do you see -- have you, in fact, from your history of the 16 instances that **Carnivore's** been used this year, have there been instances in which you captured more information that you believed you needed pursuant to a pen-register- type capture; that you believed might go into the content area and therefore you had to minimize it?

CANADY: The gentleman -- the gentleman...

HUTCHINSON: I'll just finish this and then I'll be done.

CANADY: Yes. The gentleman's time is expired. The gentleman will have one additional minute.

KERR: I'll reserve the opportunity to answer carefully after review, but there are none to my knowledge.

HUTCHINSON: So in other words, you're saying the system's working. You're not capturing content information beyond that which is intended under the court order.

KERR: That's correct.

HUTCHINSON: Thank you, gentlemen. I yield back.

CANADY: Thank you, Mr. Hutchinson.

The gentleman from New York, Mr. Nadler, is recognized for five minutes.

NADLER: Thank you, Mr. Chairman.

Forgive me if I ask any question that may be repetitive since, because of a plane delay, I arrived late to the hearing.

As I understand it, **Carnivore** can be used either for content or for, in effect, a trap-and-trace, just to know who an e-mail -- who a person is communicating with; is that true?

KERR: Yes, that's correct.

NADLER: So it can be used for either purpose?

KERR: Yes.

NADLER: Or both.

And whether it's used for either purpose depends on the nature of the court order

KERR: That's also correct.

NADLER: And it can be set either way.

KERR: It's, in fact, set specifically to meet the terms of the court order.

NADLER: Now, when you have in effect the trap-and-trace you want to know who someone is talking to; this is for past tense or for ongoing?

KERR: Basically we would capture, under the trap-and-trace and pen-register order, the to and from information. It would be recorded...

NADLER: No, no, is it past tense? You get a court order, we want to know who this guy talked to in the last two months or we want to know who he's talking to in the next two months?

KERR: It's prospective.

NADLER: It's prospective? Now, what is the difference, in terms of what you have to show -- presumably you have to show probable cause that a crime may be committed. Why would you sometimes ask to know only who he's talking to and sometimes what's being said if it's, if they're both prospective?

KERR: I'll let my colleague lead with that one please.

DIGREGORY: It depends upon the nature of the information that you have available to you at the time. You may not have enough information at the time that you seek the pen-register or the trap- and-trace order to establish the probable cause necessary to seek the order -- the Title III order for the content.

NADLER: But you have enough to -- you need a lesser standard of probable cause to get a trap-and-trace?

DIGREGORY: It's not a probable cause standard at all, it's simply a certification to the court by the prosecutor or the law -- and the law enforcement agency that the information that will be obtained through the use of the pen-register and the trap-and-trace -- or the trap-and-trace is relevant to an ongoing criminal investigation.

NADLER: With no probable cause?

DIGREGORY: With no probable cause.

NADLER: So you can get it on anybody with no probable cause?

DIGREGORY: That's correct. And I want to point out to you that this -- that the Supreme Court held, in Maryland vs. Smith, I believe, in 1979, that there was no reasonable expectation of privacy in numbers dialed by a telephone, because, essentially, when someone turns over information to a third party like the telephone company they should not have either a subjective or an objective reasonable expectation of privacy in that information.

NADLER: And does that mean that when I send a letter there's no reasonable expectation of privacy as to whom I'm sending the letter? In the snail mail. Could you get an order to the post office to tell you,

without any probable cause, who is sending me mail or whom I'm sending mail to?

DIGREGORY: We do mail covers all the time, which essentially do that.

NADLER: Without probable cause?

DIGREGORY: That's right.

NADLER: That's very interesting.

Let me ask you a different question.

DIGREGORY: May I just add one more thing, Mr. Nadler? The authority under which we operate is codified at 18 United States Code, I believe it's 31-25 (ph) with respect to the pen -- or 31-23 (ph).

NADLER: Thirty-one-twenty...

DIGREGORY: Twenty-one -- 31-21 at sect, which includes 23, 25, I believe.

NADLER: OK. Now, let me ask you a different question. You installed -- you started using this **Carnivore** system about two years ago, and no one ever bothered telling Congress about it; we just found out about it because Earthlink complained about it.

KERR: Well, no one ever bothered telling Congress in the sense of all of Congress. There certainly have been members and staff briefed on it over the last year. It's been widely...

NADLER: Judiciary Committee staff?

KERR: Excuse me?

NADLER: Judiciary Committee staff?

KERR: Yes. It's been rather widely discussed with industry, Internet service providers, other companies that provide software and hardware to the network. It's been fairly substantially briefed within the Department of Justice, including at the training center in Columbia, South Carolina, where the U.S. attorneys and AUSAs go for training. All of the major investigative programs have been briefed.

NADLER: What institutional safeguards have you set up to make sure that assurances that you've given us that information given by -- gathered by **Carnivore** on subjects not under investigation is not used?

KERR: Every time that it has been used it's gone through the internal review of the **FBI** that all such uses require. My colleague, Larry Parkinson, can speak to more detail on that.

Second, it goes to the Office of Enforcement Operations in the Department of Justice where it's, in fact, reviewed prior to ever going to a court to get a court order. So there's a very substantial level of review internal to the **FBI,** internal to the department, as well as the subsequent review of the court before an order is issued.

NADLER: Subsequent review to the court? I'm sorry.

I think I asked, once you have **Carnivore** on-line, what institutional safeguards do we have that information gathered by **Carnivore,** presumably after the court issues an order to install it, is not misused?

CANADY: The gentleman's time has expired. The gentleman will have three additional minutes.

NADLER: Thank you.

KERR: The answer to that is, that, particularly in a full- content intercept, that the information we intercept and record is provided under seal back to the court, which can itself determine that we've properly followed the order.

NADLER: It's provided back under seal to the court?

KERR: Correct.

NADLER: Is there a proceeding in the court?

KERR: I don't know.

NADLER: I mean, if there's not a proceeding in the court, it'll simply be placed in storage, no one will look at it.

PAINTER: That's not completely true, because it's placed under seal with the court in the Title III content intercept. And then at some time in the future, the court can, under Title III, make that available to, for instance, the person whose conversations were intercepted and/or his defense counsel.

NADLER: Now the person -- if a person has been the subject of such an order and his content has been intercepted or simply -- or simply that whoever he was e-mailing to has been made known to the **FBI,** and it's determined that this person should not be subject to any charges, did nothing wrong, is he ever made aware that his privacy was so violated?

PAINTER: Under Title III -- under the provisions of Title III at -- if a Title III order is denied by the judge or if it expires, after a certain period of time -- I believe it's 90 days -- there has to be notice to the people whose conversations were intercepted. I think that's been done very broadly, as I understand it.

NADLER: So people's whose conversations were intercepted or whose -- or on whose e-mail there was a trace, are eventually told?

PAINTER: Under the provisions of Title III, when you're dealing with content, yes, that's correct.

NADLER: And what about when you're not dealing with content, when you're dealing with a trap-and-trace?

PAINTER: Well, again a trap-and-trace -- and I should emphasize something that Mr. DiGregory said earlier, the trap-and-trace, the reason probable cause is not required, is this is a very preliminary investigative step. It is really, literally, the addressing information and nothing more. And it's...

(CROSSTALK)

NADLER: I understand that, but if you've -- without probably cause to believe that I've committed a crime or done anything wrong, but simply as part of an investigation, you have followed who I'm talking to by e-mail or for that matter, not by e-mail, you put a trap-and-trace on my phone for the last six months, now you've determined that there's nothing further to investigate, do you ever tell me that my privacy was violated in that way? Do I ever know about it?

DIGREGORY: I don't believe that there is any requirement for disclosure in the law. And I would only -- I understand that you're using the term "that my privacy was violated" and only relying upon the case law, which indicates that there's no reasonable expectation of privacy in such information, I just wanted to make that point yet again.

NADLER: Well, that may be from the Supreme Court's point of view, that there's no reasonable expectations of privacy, but I think as a practical matter, most people would be somewhat upset if they thought that someone was following exactly who they were talking to on the telephone or who they were mailing e-mails to.

But be that as it may, from a legal standard that may not be, but the fact is there was -- in a practical sense, there was an invasion of privacy, government gathered information that maybe I didn't want people to know, I think I should know about that. And maybe I should be able to say to the government, On what basis did you do this? Did you have any reason to do it? And maybe they did and maybe they didn't. But right now, there's no provision for that.

PAINTER: Well, that they -- first of all, the prosecutor has to certify to the court that it is relevant to an investigation. And then second, it's that class of information alone, and it's limited to a period; it can't be done ad infinitum. A trap-and-trace order...

NADLER: What period is it limited to?

PAINTER: ... is 60 days.

NADLER: Can it be renewed?

PAINTER: It can be renewed, but it has to go back to court.

NADLER: How often can it be renewed?

PAINTER: I'm not sure there is a limitation.

NADLER: What's the longest anyone has ever been subject to this?

PAINTER: We'd have to look into that to be sure.

NADLER: Has anyone ever been subject for more than, let's say, a year?

PAINTER: Again, I don't have that information available at this point.

NADLER: Five years? Could you rule that out?

DIGREGORY: I mean, I don't -- if you want us to try to find out the longest time that anybody has ever been subjected, we can try to do that. I don't know if we have those records, but we can try to do that.

NADLER: Thank you, Mr. Chairman.

CANADY: Thank you.

The gentleman from Alabama is recognized for five minutes.

BACHUS: Thank you.

The potential for abuse here is tremendous. Would you all agree?

PARKINSON: Congressman, I guess I don't agree with that.

BACHUS: All right. And you don't have to give an explanation.

PARKINSON: Well, I think at a certain point in time we have to rely on the good faith of public servants who are -- who have a number of checks and balances in case they get try to get away with something.

BACHUS: I think you're exactly right. I think what you're saying is, trust us. You have to rely on us.

And what that reminds me of is these IRS agents who used information to check up on their ex-spouses and their boyfriends and their girlfriends and potential adversaries for affections and, you know, all that we've heard for really years and years and years -- J. Edgar Hoover, what he did.

But let's talk about those checks and balances, because I think you're exactly right. I think you have to rely on -- you certainly have to rely on that, because -- you can't go to AT&T today and say, "We're going to analyze all the phone calls that come through your system," can you?

KERR: That's correct. We can't do that.

BACHUS: But you can do that with this -- with **Carnivore**, with...

KERR: No, we, in fact, specifically don't do that. We only...

BACHUS: I know, but you do have to analyze -- or you do have the ability to analyze everything coming through that information stream, don't you?

KERR: No. We, in fact, restrict what we...

BACHUS: Now, you restrict it. But you have the ability to monitor...

KERR: No, we don't. We don't have a system with the capability to do the real-time processing of that much information.

BACHUS: You don't have time -- but you can move it around and just capture whatever you want on that system. I mean, you don't have the ability to go to a telephone...

KERR: We don't have the right nor the ability to just go fishing.

BACHUS: Well, you have the ability to monitor anything within that information stream.

KERR: No, we, in fact, have the lawful opportunity to...

(CROSSTALK)

BACHUS: No, I said you have the ability...

KERR: ... some very specific information...

BACHUS: No, no, no. OK. You might not have the -- you say you don't have the legal ability. But you have the technology to monitor that information stream, anything in it.

KERR: We are not sitting looking at the information stream and moving our filter around. It's, in fact, put in place with a court order. It's not intended...

BACHUS: But you have the technology to go in and monitor every one of those e-mails on the system, if you wanted to. Not all of them at once, but you could just -- you could monitor here, you could monitor there...

KERR: Certainly, if you had access to the system, in principle, you could do that.

BACHUS: Which you do -- and you can't with telephone calls.

KERR: Well, in fact, depending on where you are in the telephone system and what kind of switch you're in, you might be able to do a great deal.

BACHUS: So, you...

KERR: But again, it's the same thing. Remember, the big telephone switches are simply computers as well, and so if you got into one, you presumably could see a lot of traffic.

BACHUS: OK.

KERR: The fact is that there are a lot of bars to our doing that, starting with the law.

BACHUS: Safeguards. They're safeguards.

KERR: What?

BACHUS: They're safeguards. They're safeguards.

KERR: It's the law. It's illegal to do that.

BACHUS: The law. OK. I mean, it's the law. That's one of the checks and balances and safeguards.

KERR: Correct.

BACHUS: Now, one of those was, you said, the Justice Department. You have to go to the Justice Department for -- and notify them and get their approval.

And you said that it takes a higher level of authorities there to get approval for your activities; is that correct?

KERR: What Mr. Parkinson was saying is that for the trap-and- trace and pen-register, which only allows addressing information, it's a different level of review, but to get content where probable cause needs to be demonstrated...

BACHUS: You have to go higher up.

KERR: It, in fact, takes high-level approval in the Justice Department before we are ever able to go to the court.

BACHUS: Well, let me ask you this: Why did Janet Reno not know about this, although it's going on for three years, and she is, in fact, the attorney general?

KERR: Well, I would remind you that the Department of Justice is some 127,000 people...

BACHUS: OK.

KERR: ... and multiple investigations.

BACHUS: No, I think -- I think that's a valid point. There are 127,000 people over there, and we might have...

DIGREGORY: I believe that Attorney General Reno said that she'd known about the capacity to do this. She was interested in taking a closer look at the systems application and implementation...

(CROSSTALK)

DIGREGORY: ... to ensure that we're balancing privacy and law enforcement needs, and I think that's what's going to happen with respect to this independent...

BACHUS: So she didn't about the...

DIGREGORY: ... verification and validation.

BACHUS: How about Echelon? It's our understanding that the National Security Council testified before Congress and said that they routinely shared information they gathered with Echelon to law enforcement agencies. Do they share information with the **FBI?**

KERR: What you're referring to, of course, is whether the National Security Agency...

BACHUS: I mean, through their Echelon programs, do they...

KERR: Through their various intercept programs may, from time to time, appropriately share information with law enforcement. But there're, in fact, some very important hurdles there, including the Classified Information Protection Act and others, so that, in fact, the primary purpose of a system may have been intelligence collection. Incidental to that primary purpose, it may have collected important information about a crime, either committed or being planned, and there are mechanisms to take advantage of that.

CANADY: The gentleman's time is expired. Without objection, the gentleman will have three additional minutes.

BACHUS: Echelon, as I understand it, they monitor -- they can monitor all telephone calls, all e-mails, all faxes; is that your understanding?

PARKINSON: I think we should defer to the National Security Agency to talk precisely about Echelon. I don't think we're prepared to talk about it today.

BACHUS: I guess I would just ask the FBI. They do share -- you say they -- when he said they routinely shared information with law enforcement agencies, do they share information with the FBI?

PARKINSON: We have, as you probably know, a very significant national security responsibility in addition to law enforcement. So it not uncommon at all for the National Security Agency to selectively share pieces of information that it may acquire. But it does so, as Dr. Kerr pointed out, with significant hurdles and legal constraints.

BACHUS: I think you've raised a good point. I'd like to use that as my final question, and that's -- you say the National Security Council. I think we all presume they're dealing with national security. But then they gain information on another subject. I mean, if it's national security, obviously they could share it with you. But let's say it's another subject. Or let's just say that we're talking about Carnivore -- what's the name of it?

DIGREGORY: Carnivore.

BACHUS: Carnivore, OK. Now the examples you gave us were about espionage or terrorism. But do you use this, say, in antitrust investigation? Would you use it in income tax evasion cases? Can it be used in, say, OSHA investigations, or EPA violations? Are there any restrictions there?

KERR: It would, of course, have to be a federal felony to come under Electronic Communications Privacy Act.

BACHUS: And all those are ...

KERR: And it would have to be, in fact, one of the predicate offenses under Title III to come under those authorities.

So, no, it's not every offense. Clearly Internet fraud would be an appropriate target. Child pornography on the Internet would be an appropriate target. These are major programs within the FBI that we would...

(CROSSTALK)

BACHUS: Can you -- other than e-mail, can you get into files? Can you -- do you have the ability to get into someone's files?

KERR: We have, in at least one case, been able to intercept, using a different protocol -- file transfer protocol, but with relatively small files. We can only get at what we have the addresses for within the protocol that's being employed.

BACHUS: But once you have that and the passwords, you could actually get into maybe a mainframe or someone's database?

KERR: No. We're only authorized what the court order says. It's not a matter of going and doing exploration or surveillance with the tool.

WATT: Will the gentleman yield for a second?

Does that extend to e-mails that have already been transmitted? If you had the address, would you -- would you have the authority and/or the capacity to go in and either look at the content of a prior e-mail or look at the number or instances in which there has been communication to deliver that e-mail?

CANADY: The gentleman's time has expired. The gentleman will have one additional minute.

BACHUS: Thank you.

Let me -- after he answers it, may I have my minute then?

KERR: Shall I try to answer Mr. Watt's question?

BACHUS: Answer his, yes.

KERR: OK. The Carnivore system basically deals with message traffic on the fly. If the messages have already been sent and received, another way we, for example, might get it would be if, for example, a search warrant were offered and we seized a computer and we found the messages on the hard drive of that computer. Or, as one of the members of the subcommittee pointed out, deletion doesn't necessarily mean deletion. We can, in fact, sometimes recover messages even though they have been thought to have been deleted. And we have a unit that does that. But they work under a more normal search warrant environment.

DIGREGORY: And under certain circumstances, stored communications that are held -- stored e-mail communications held by ISPs can be obtained by search warrant as well.

BACHUS: All right. Here's my final minute. You mentioned...

CANADY: The gentleman will have one additional minute.

BACHUS: You mentioned judicial oversight. And, Dr. Kerr, you mentioned that you've got the defense attorney and he's looking over our shoulders; you have the judge, he's looking over our shoulders. And obviously if the defense attorney has the ability to do that, that is a pretty potent weapon in limiting what you do.

But are you saying, when you say that, that all these cases are ongoing criminal cases in court where there is, in fact, a defense attorney? Or could it be -- what about a case of an investigation where there's no attorney or not active court case?

KERR: I think Mr. DiGregory pointed...

BACHUS: Or can it be used in those cases?

KERR: ... out the provisions of Title III that would lead to judicial notice of those who had been intercepted. They certainly, at that 60- or 90-day point, having been informed that their communications had been intercepted, would take a great interest, with or without their attorney, so I think that the system is oriented very well to protect their privacy and rights.

BACHUS: Are you unable to take information you gain from these investigations and pass them on to other law enforcement agencies about unrelated investigations? Or is that information off limits?

CANADY: The gentleman's -- I'm sorry, the gentleman's time has expired. The gentleman's had more time than anyone else. We're going to go to -- we have a limited amount of time. The members of the panel can answer a written question about other things the gentleman might want to ask, but Mr. Barr's entitled to have his time.

So Mr. Barr is recognized.

BARR: Thank you, Mr. Chairman.

This is actually quite fascinating. The Clinton administration is fascinating. It never ceases to amaze me. For over -- for almost a year now at the other end of this very hallway, in the Government Reform Committee, we've been having a series of hearings, the conclusion of which, from the Clinton administration standpoint is, we don't even know how to keep track of our own e-mails. And now we have a very sophisticated system for tracking other people's e-mails.

BARR: The fact of the matter is, I think they know exactly what has happened to their e-mails and they know exactly what's happened. I just think that we have two different directions for the Clinton administration: When they want to protect themselves, they have one standard; when they want to get information out of other people, they have quite a different standard.

And the fact of the matter is, with all do respect, simply because there is a privacy act or simply because there are sanctions in Title XVIII for misuse of the Title III provisions does not guarantee that nobody in this or any other administration will abuse it. So I think we really need a little bit more than simply saying that there are provisions in the code.

The problem that I have with Carnivore, several problems, but the fact of the matter is Carnivore is not a passive system: It doesn't sit there like a basket and these e-mails just sort of drop into it. It is very much an active system. And it has to have some mechanism for scanning the information in that ISP stream in order to pull out what the court order allows you to pull out.

The problem -- let me ask about two things, though, that are particularly problematic. As you all have testified earlier, with regard to Title -- Chapter 206 of Title XVIII, which are all of the provisions that we've been talking about that govern trap-and-trace and pen register, you're doing something very different here, and that bothers me.

With traditional trap-and-trace and pen registers with phone numbers, as you all have testified, you get an order -- granted the threshold is substantially lower than a Title III and we understand that -- you get that from a court -- a court has to grant it, there's no discretion for the court -- and the telephone company, as it were, has to comply with it. They can't say -- they can't just, you know, give you the high-hat and say, "We're not going to do," they have to comply with it. And you tell them what you want and they give you what you want. And if they don't then you can bring sanctions against them, because they are required under the statute to do that. You're doing something very, very different here.

What you're doing here is, you're going to that ISP provider, which stands in the shoes of the traditional phone company when you're looking at a traditional hard number trap-and-trace or pen register, and you're saying, We're not satisfied with what the statute says that you have to install this and give us the information. We don't trust you. I don't know why you, you know, what your rationale is, but you're saying, What we're going to do is, we're going to go outside of the law here, basically, and we're going to force you to allow us to put our software into your system. You will not be able to monitor it. It's completely unsupervised and we're then going to take it from there. Thank you very much guys; you just give us access and we'll do our thing. That's very different from the way trap-and-trace and pen registers work under the traditional Chapter 206 scheme.

Also -- I think also, there is new legal ground that you all are trying to break here and establish the precedent that I don't think is existing anywhere in federal law or case law -- now, I know you're trying to make it in the Earthlink case -- where you're saying you have the authority to go in and, sort of, harvest large quantities of information and you'll filter out what you want.

I think those are two very, very large steps that we're taking here. I don't think this has been well thought out. And that's two areas that I have concern about. Why is it not sufficient -- because we have both testimony, as well as a number of articles that indicate that Internet service providers have indicated, and I haven't seen anybody refute it, that they can do the very same thing that Carnivore does, but do it in a much -- in a way that is much more protective of the privacy of the Internet service provider users.

And, certainly, if you would go to Earthlink, for example, and say, "This is the information we want," the same as you would do with the phone company for a trap-and-trace or a pen register, they're obligated -- they would be obligated to give that information to you, and if somehow you had evidence that they were not doing it or that they were not capable of doing it, and I don't think that's the case, then you could seek sanctions against them.

Why is it, in both of these areas, you're trying to break new legal ground?

BARR: What is it that's insufficient that you don't like about the existing statute that you're willing to operate within the bounds of it?

PAINTER: Let me answer with respect to that last point whether or not there's been cases where the Internet service provider could not provide the information, and Dr. Kerr can talk about this as well.

There have, in fact, been cases -- in one case, without mentioning who the provider is, in fact the Internet service provider was not able to provide all of the information. In that case, in fact, it wasn't just a matter of them saying, Well, we have to comply with a court order. They went back to the court, there was a proceeding before the court, all of these issues, including the issues about too much material being grabbed by this program -- or that was at least the argument that was raised -- were raised with the court and the court ordered this device be put in place.

BARR: And that was not the Earthlink case?

PAINTER: Again, since that was an ongoing criminal case, I don't want to mention who the Internet service provider...

BARR: Well, let's not play niceties here. I'm asking, was that the Earthlink case, because that's been reported in the newspaper, it's not some great dark secret. And I think you are describing the Earthlink case.

PAINTER: I think the problem is this is an under-seal proceeding, there is a court order in that proceeding, I don't want -- because it's an under-seal proceeding we could talk about the public facts that were argued at the hearing, but I don't want to mention the name of the provider.

BARR: I thought you said at the beginning it wasn't the Earthlink case.

PAINTER: I did not say that. I said I don't want to...

(CROSSTALK)

BARR: I think it is.

PAINTER: But in fact...

(LAUGHTER)

PAINTER: But in fact, in that case, there was not complete information given because only the outgoing -- or the incoming messages were trapped but not the outgoing messages, and there was some evidence to

that effect that was presented to the court in the form of affidavits...

(CROSSTALK)

BARR: But that's very different from the testimony that we've had from Earthlink.

PAINTER: And what I was going to say is it's certainly the policy, as I understand, at the FBI and the preference that if, in fact, the Internet service provider can provide that information and do it in a timely fashion, that's what they'd prefer. It raises this sort of example.

CANADY: The gentleman's time has expired. Without objection, the gentleman will have three additional minutes.

BARR: Thank you.

Are you saying, then, that in every one of the 25 cases in which Carnivore has been used, the only reason that it has been used is the Internet service provider has told you they cannot provide the information that you need?

PAINTER: That is my understanding, and I defer to Dr. Kerr to also address that.

KERR: I think that that's generally the point. In fact, our favorite outcome is that, if the Internet service provider can, in fact, provide the information to us covered by the court order, that that's what we would like to do. And there's some very large Internet providers not too far from here, who have the entire capability to do that.

At the same time, in some of the over 10,000 ISPs around the country you'll find some that have very limited technical capability, their capital structure is very small, they're not in a position to buy equipment and set up a capability for us that may only be used once in the entire business history of that company. In those cases where they can't preform, we're prepared to take the technical and cost risk away by bringing in our Carnivore system and employing it.

BARR: Here we go again. I guess what you're telling us is Carnivore's, sort of, the privacy advocate's best friend, that it, you know, hey, we -- I mean, do you have ISPs breaking down your door and saying, "Please install Carnivore"? I don't think so.

Is there any specific statute or case law, other than perhaps the Earthlink case, which is currently pending as I understand it, that provides authority for the government to go to a provider of electronic information, a telecommunications firm, and say, "Give us everything you have and we'll filter out what we have"?

That's very different from the traditional rationale underlying both Title III and Chapter 206, which is the government can't go in and just harvest everything on its own and then filter it out; you tell somebody exactly what you want and that's all that you get.

DIGREGORY: In the case to which -- in the case referred to by Mr. Painter, we successfully relied upon

the pen-register statute. And know of -- and I stand corrected if someone has a correction to make -- and I know of no other case where an ISP has challenged our reliance on that statute.

BARR: No, but is -- what I'm saying is, is there any statute or case law other than this one case, that as I understand it is still in litigation?

DIGREGORY: And I'm saying we've relied on the pen-register statute successfully in this area...

(CROSSTALK)

BARR: So you -- the Department of Justice...

(CROSSTALK)

DIGREGORY: ... and there have been no other challenges other than the one mentioned by Mr. Painter.

BARR: The Department of Justice position is that Chapter 206 provides statutory, therefore, also constitutional authority, I guess you would argue, that you had -- that the government has the authority -- the right to go in and harvest a large category of information, far beyond simply the target, and then itself take out the targeted information.

CANADY: The gentleman's time has expired. The gentleman will have one additional minute.

PAINTER: I think when you use the term harvest, you're using a term that really doesn't apply here. That's not what it's doing. It is only harvesting, it is only capturing the information specifically that you allow and the court order has mandated.

BARR: But in order -- I mean, this is sort of -- that's what I love about the Clinton administration, then you get into this circular argument, it's almost metaphysical. You have to have some way of going in there and finding what you're looking for, otherwise it's a non-sequitur.

KERR: Let me, as the -- part of the non-political agency here, try to answer your question directly. What do we actually do in the **Carnivore** system?

What we do is, we first ask the ISP to bring us the smallest part of the message traffic that would contain the target messages. We then bring it to an interface, where, in fact, a clone of that reduced set is made. The regular message traffic goes on, unimpeded, to the legitimate recipients of it. We then filter the cloned stream of information and the packets that do not pass our filter, because we're not allowed to record them, in fact, vanish at that point. The only thing that passes our filter are the packets with the appropriate addressing information to meet the court order. And I think we've demonstrated that a number of times.

In fact, we appreciated your visit, some months ago, when you saw it. As to...

(CROSSTALK)

BARR: When I saw what?

KERR: When you were at Quantico, some of the demonstrations we gave you, were, in fact, of these capabilities.

BARR: That was years ago. That was on CALEA. That was like, four or five years ago, that had nothing to do with **Carnivore.**

KERR: Well...

(CROSSTALK)

BARR: Well, I hope it didn't, because it wasn't described to me as **Carnivore.**

KERR: Hadn't been named yet, perhaps.

But the point is that we're not scanning the full message traffic passing through an ISP. In fact, to do it effectively we want to use the smallest subset of that. A very sophisticated, larger ISP will, in fact, give us the ultimate subset, which is the target messages, and we would have to install nothing.

In some cases, we have to provide technical assistance by putting our system in the ISP in order to do that final filtering.

CANADY: The gentleman's additional time has expired.

I want to thank all the members of this panel for your testimony. I think we've had good presentations in your testimony. And the questioning period has been, I think, very helpful.

We will have additional questions, as I indicated in the outset, and we will do our best to send those to you very soon. And I would ask that you do your best to respond to us within a very short period of time after you receive the letter of which we will send with the questions. Again, we thank you for your testimony and your assistance to the committee in this oversight responsibility.

And now we'll move to our second panel. And I would ask that, as people are exiting the room and coming into the room, to try to be as quiet as you can, because I'm going to proceed with the introduction of the members of the second panel as they are coming forward to take their seats.

The witnesses on this second and final panel of today's hearing will discuss privacy concerns and concerns for network security raised by the use of **Carnivore.**

Our first witness on this panel will be Barry Steinhardt. Mr. Steinhardt is the associate director of the American Civil Liberties Union.

CANADY: Next we will hear from Alan Davidson, who is the staff counsel for the Center for Democracy and Technology.

Following Mr. Davidson, will be Tom Perrine. Mr. Perrine is a principal investigator for the Pacific Institute for Computer Security. He is also the manager of security technologies for the San Diego Super Computer Center.

Robert Corn-Revere will then testify. Mr. Corn-Revere is an attorney at Hogan and Hartson, specializing in First Amendment, Internet and communications law. Mr. Corn-Revere is also the co- author of a three-volume treatise entitled, Modern Communications Law. We have heard from Mr. Corn-Revere on this subject previously.

Following Mr. Corn-Revere will be Matt Blaze, a research scientist at AT&T Labs. Mr. Blaze specializes in the architectural aspects of security and trust in large-scale computing and communication systems.

Stewart Baker, an attorney at Steptoe and Johnson, will then testify. Mr. Baker represents major telecommunications equipment manufacturers and carriers in connection with the Communications Assistance for Law Enforcement Act and law enforcement intercept requirements. Mr. Baker was the general counsel of the National Security Agency from 1992 to 1994.

Finally, we will hear from Peter William Sachs. Mr. Sachs owns ICONN, LLC, a small Internet service provider based in New Haven, Connecticut.

I want to thank each of you for being with us here this afternoon. I would ask that each of you do your very best to summarize your testimony in no more than five minutes. Without objection, your written statements will be made a part of the permanent record of today's hearing.

So we will now turn to our first witness of this panel, Mr. Steinhardt.

STEINHARDT: Thank you, Mr. Chairman.

I want to thank the committee for the opportunity to speak here today. I'd also want to thank you for so expeditiously calling this hearing.

As I think the prior testimony made clear, we are dealing with an extremely important issue, and one that bears a great deal of scrutiny, more scrutiny than even this hearing will allow for.

Let me begin to put **Carnivore** into some context. To my knowledge, **Carnivore** is unprecedented in the history of domestic communications surveillance. Never before has law enforcement installed a device which accesses all the communications of a service provider's customers, rather than only the communications of the target of a particular order. Never before has a law enforcement agency claimed that it should be granted access to all communications passing through a service provider's network based

on an unsupervised promise that it will not stray beyond the confines of its authority.

Carnivore is roughly equivalent -- as a number of the members have suggested, it's roughly equivalent to a wiretap, capable of accessing the conversations of all the phone company's customers or to use the analogy that was offered before, when it suggested that the to and from which the **Carnivore** box uses as the key to look for which messages to record, the analogy of a letter, this is the equivalent of going to a post office and stationing an **FBI** agent there, looking at the addressing information of every letter that goes through and then picking out those which it wishes to record either the addressing information or to open up and actually look at the content.

Now I must say, I want to comment on one thing in this section -- one thing that you were told about earlier this morning, and that's this audit trail that for the first time we've heard about -- this audit trail which apparently we are told records at least what the filter settings are and some of the traffic information.

I think there are probably a number of things that are worth noting about this audit trail. First, this apparently was created only recently, and I would suspect created only after the public disclosure and discussion of **Carnivore.** But, secondly, I think it's worth noting about the audit trail, is that it's only of use in a very limited number of cases, that it really provides very little in the way of assurance.

It's, for example, not available in cases where there is a trap- and-trace or pen-register order. Who is going to look at this? They're not required to turn over even the audit trail to a judge.

It is, as a number of the members suggested earlier, not particularly helpful if the conversations or the addressing information that has been recorded -- picked up, is of an innocent third party, not the subject of the order, not someone who's being prosecuted.

STEINHARDT: They don't have a defense attorney, they don't have an opportunity in which to contest that. I think that what the discussion about the audit trail suggests is that you need to look very, very carefully at all these details.

It's hard to imagine how the operation of Carnivore can be squared either with the Fourth Amendment or ECPA, which was adopted to implement the Fourth Amendment in the context of electronic surveillance.

The very premise of the Fourth Amendment is that searches should be narrow and targeted so as to avoid the intrusion into the privacy of persons who are not engage in a crime or for whom law enforcement does not have reasonable cause to believe that they are engaged in a crime.

In recognition of this, ECPA requires the government to specific the person who's the target of the investigation, crimes under investigation, the particular systems from which the communication is to be accessed. They place on the provider of the communications medium the responsibility to separate out the communications of persons authorized to be intercepted from other communications.

Law enforcement is required to minimize the inception -- the interception of non-incriminating communications of a target of a wiretap order. **Carnivore** is not a minimization tool, as been suggested. **Carnivore** is in fact a maximization tool because it is capable of giving law enforcement access to the entire stream of communications that is traveling through the service providers' networks.

Now, I think it's fair to say -- and I urge you not to take the leap today to think that this is a settled question. I think it's fair to say that the Congress never contemplated or authorized a wiretapping scheme that allowed law enforcement to access everyone's communications, that had the potential to access an unlimited number of communications, only a small fraction of which involve criminal activity, and that targeted entire communications network rather than a particular person's communications.

The questions Mr. Barr asked are exactly the right questions. What is the statutory authorization for **Carnivore**? What in the statute, what in ECPA, what in the Constitution gives law enforcement, gives the **FBI** the authority to insist that a service provider install **Carnivore**? I think that's an extremely important question which is not answered by one case, which we know very little about other than the back and forth in the public and to some extent before this committee -- that we know very little about and that never went higher than one federal magistrate.

Now, the **FBI** has two responses to the concerns that have been raised by **Carnivore.** First, they assure us that they can be trusted to strictly adhere to the Constitution and statutes. Second, they argue that they're being hamstrung by new technologies and that **Carnivore** is necessary to conduct successful investigations. Let me first address the "trust us" argument.

The **FBI** has a very checkered past when it comes to fidelity both to the Fourth Amendment and First Amendment rights of Americans. As a number of you pointed out, we all know about the wiretapping of Martin Luther King and other leaders of the civil rights movement and the more recent cases where there has been illegal surveillance of political figures.

But even if you assume, for the sake of argument, that **FBI** officials, **FBI** agents are not going to engage in a bald criminal violation of law, I think you need to look at the recent history of the **FBI,** which tells us that -- the recent history tells us that the **FBI** cannot be expected to keep its promises on communication surveillance history. Recent history tells us that we can fully expect the **FBI** to push the envelope of the wall -- as they have done in this case by pushing the envelope of the trap-and-trace laws, for example, to claim that **Carnivore** is a permissible result -- and to eventually break out of the envelope of the law.

Let me give you -- let me give you some examples.

I think best example -- and I detail this in the appendix to my testimony, I go through a good deal of this history, but let me give you one example. When Congress passed the Communications Assistance to Law Enforcement Act that was referred to here earlier today, CALEA, in effect a bargain was struck: In return for requirements that new networks be constructed to preserve the then-existing capabilities for law enforcement, law enforcement, the **FBI** in particular, agreed not to use the new law to force service providers to provide it with new surveillance capabilities or with greater capacity than then existed.

Simply put, the **FBI** has not kept its end of the bargain. The CALEA implementation process has been characterized by an **FBI** power grab. As I detailed in my -- in the appendix to my testimony, the **FBI** has consistently sought greater capacity and new surveillance features than existed in 1994. In some cases it has sought capabilities that were specifically promised to the Congress that they would not seek.

Now, I will only given one example of this. Others are in my testimony. But I think this example is worth fastening on for the moment.

When CALEA was considered, the FBI explicitly told the Congress it would not use the new law to seek to turn cellular telephones into location tracking devices.

STEINHARDT: Director Freeh testified that, quote, "There is no intent, whatsoever, with reference to this term" -- parenthetically this term meant call set up information -- "to inquire anything that could properly be called tracking information."

Well, whether or not that was Director Freeh's intention in 1994, it quickly became the FBI's policy in 1995. And the FBI has fought tooth and nail -- first with the cellular telephone industry, then with -- before the Federal Communications Commission, and now in the U.S. Court of Appeals for the District of Colombia, fought tooth and nail for the proposition that CALEA, in fact, does require the cellular operators to provide it with location tracking information.

Now, on the question of the supposed new circumstances that require Carnivore, first, you're going to hear testimony from the Internet service providers here today and you've already heard a good deal from them in the press, that they are willing and able to provide law enforcement with a narrow targeted set of communications to which law enforcement is entitled.

They can perform the segregation of communications that is the equivalent of providing access to dedicated line; there is no need to resort to Carnivore. And I urge you not to simply trust on faith the suggestions of the witnesses that you -- that you heard earlier today, that there have been cases that other service providers cannot provide them with that information.

Once again, we're in the position of, "Trust us, we know how this black box works," or in this case, "We know that the service providers cannot give us this information without resorting to this black box." The only case that we know anything about in detail, and not many details, because these matters are all under seal, because these cases all come up ex parte -- these request for orders come up ex parte, is Earthlink.

And it was quite clear this morning -- this afternoon, rather, that the witnesses from the government were not prepared to ask you to do much more than trust us, there are cases.

CANADY: Mr. Steinhardt, you're now at 10 minutes. So if you can conclude, because -- let me just explain to all the members of this panel. This subcommittee has another hearing. That's not minimizing the importance of this in any way, but we do have a hearing on a proposal that Mr. Frank has introduced, which we are moving to after this.

So to the extent that you can really stay close to that five minutes, it would be beneficial, given the size of the panel.

FRANK: Mr. Chairman?

CANADY: Yes?

FRANK: Is it the intention of the chair to adjourn this hearing and go to the next one at 4?

CANADY: It is the intention of the chair to hear the witnesses and to have one round of questions, and then go to the next hearing.

FRANK: Thank you.

STEINHARDT: Well, I'll stop there, and allow the rest of the panel to speak, then.

CANADY: Thank you, Mr. Steinhardt.

Mr. Davidson?

DAVIDSON: Hi, I'm Alan Davidson, with the Center for Democracy and Technology. I'd like to thank the committee for holding this hearing, and commend you for your continued thoughtful exploration of the Fourth Amendment and cyberspace, a very important issue today.

CDT is a civil liberties group, and we're concerned about **Carnivore** for at least two reasons: first, because **Carnivore** itself, as it's implemented is very problematic; and, second, because **Carnivore** raises broader issues about the need for greater privacy protections in our increasingly outdated statutory and constitutional framework that governs our surveillance and privacy laws.

Just to start with the first, the questions about **Carnivore.** I think the threshold question for **Carnivore** is that it has -- **Carnivore** has access to much more information than it is legally entitled to collect. How do we know that we can trust **Carnivore?** How do we know what kind of leash has been put on **Carnivore?**

I'd like to, with the committee's indulgence, try to give the committee a sense of a little bit of what we're talking about with packets, here. I've got a couple of slides that I'd like to put up quickly.

Let me just give a couple of disclaimers. These are captures of actual real packets. And for those who didn't bring their opera glasses, these are actually -- should be in your packets. They're the -- and for folks in the audience -- they're the last three pages of my testimony.

These are examples of real packets that have been captured from CDT's network with a very crude tool. That's a tool that may not look anything like what **Carnivore** looks like, but I thought it'd be helpful for the committee to at least get a sense of what some of the things that we're talking about look like and how hard it is to do some of the things that **Carnivore** says it's doing, and how hard it is, maybe, to trust **Carnivore.**

DAVIDSON: And to start with, this first packet is a sample e- mail message -- actually a real e-mail message that I sent to Paul Taylor, subcommittee counsel, on Friday and was captured off of our web site -- off of our network.

What's interesting -- this is what a packet sniffer does to a packet. It, kind of, breaks it up into different pieces that can be understood. And there are, sort of, really -- sort of two chunks to this information. The first chunk is the stuff at the top, which a lot of people call the header information, which contains a lot of the addressing information and description of the packet. The second half of it is what I call the data part, or the payload of the packet. And that includes the data, the text, the content, if you will, of what we're

talking about.

And so in the context of this message, there's actually a very simple answer if we're talking about a pen register and we want to know the tos and froms, the origins and destinations, the numbers, if we're going to extrapolate pen registers onto the Internet, there actually is, sort of, a very simple answer at the top here about where this packet is coming from and where it's going to. It's that first address, which is the yellow address, 207226, which actually happens to translate into the computer at CDT that I was using. And then there's a destination address which is in red there, which is that 216 address that happens to be CDT's mail server.

And that; if you just took it on its face, would be the very simple header information -- the numbers of the address that it's coming from, the address that it's going to.

What we're hearing about **Carnivore** is actually **Carnivore's** trying to do something a little bit more subtle, trying to get more information. The problem is, this is kind of difficult on the Internet because origin and destination is very context-dependent. It depends on where you are on the network, and what level of the protocol step -- what you're trying to do within the -- where you're looking within the packet.

And so in this case, it's an e-mail message. And you can see that the content of the e-mail message includes the line, "to Paul Taylor, mail that has the come from Alan Davidson." That's the to and from information that the **FBI** is seeking to get. And so what **Carnivore** really needs to do is dig in to the content of this packet, analyze it, and ferret out this to and from information which is what the **FBI** says they want to get.

And I raise that just because, to think that this is a simple thing; to think that this is just information that's sitting on the top here and we can just pull off, is not to get the concept here. I think it's a very subtle thing, it's a very difficult thing, and it requires a lot of analysis.

Let's just skip real quick to that -- well, there's a second example which is an example of Chairman Canady's web site -- a similar situation. There's a to and from IP address at the top, but to actually get a look at what site I am visiting, what is the destination of this traffic, you have to look into the content of the packet. In this case, www.house.gov is the server, the host, and Canady p. 74 is the -- is the actual page that I was looking at at the time.

Now it's reassuring that the **FBI** says that they are not -- that **Carnivore** right now does not actually seek out URLs, the web sites that people are visiting, but if one's going to extrapolate this notion of numbers dialed into something that lets you get the origin and destination of Internet communications, it seems reasonable that this is the next thing they're going to look for.

And that becomes even more problematic. If you can go to the third slide, very quickly, I know I'm running out of time, this is a copy of a web packet. This is a web search that we do that looked at BarnesandNoble.com's web site. I did a search for a book -- this happened to be a book on prostate cancer, for no other reason than my personal interest -- someone in my family -- and I just wanted to show you what the URL looks like for this.

If the **FBI** continues this extrapolation and says, We just want to capture the URL, not the -- again the source and destination IP address at the top, but the URL of the web site destination that I'm visiting, they get a lot of information. They get this host in purple, which is shop@BarnesandNoble.com. They also get the page that I'm looking at, which is a book search, that is for prostate and cancer. You can imaging, this could be -- you know, I could be looking for all sorts of things. I could be looking for sites about religious

topics, or political topics, or social topics, and all of this gets listed in this pen register for the Internet.

And so, I think -- I realize I've gone over my time already here, but I think the point that I'd like to try to make is that, you know, some of these things, these rules that we've come up with, like pen registers, we came up with in the old context, the telephone context, for example. And the idea that digits dialed were something -- was something that wasn't as sensitive was what drove, I think, Congress to create this extremely low standard for access.

DAVIDSON: And I think Congressman Nadler's really on to something when he questions what the standards are. There's a very big difference between a reasonable -- I mean a relevant standard and a probable cause standard in the pen-register context.

And I think there's a greater example -- so, when we talk about **Carnivore,** we've got a lot of concerns about how it's being used. I would just summarize to say we are concerned about the fact that it needs to be opened up for the world to see. There needs to be an open source methodology used here so that we know exactly which pieces of the packet **Carnivore** is looking at and how it's doing its searches.

Second of all, we think that there ought to be a bit more control in the hands of the ISP. The ISPs are the people who are in the best position to do this balancing test.

And, finally, I think all of this points to the need for Congress to revisit some of these basic protections. The question of whether or not the pen register should be applied to the Internet is just the tip of the iceberg. The home has exploded; there's all sorts of information that used to be kept in the desk drawer that's now being kept out on the network. The law does not protect that information well. We need to revisit this.

The White House has taken a good first step. We're looking forward to working with everybody. That step doesn't quite go far enough, but we really want to work with folks to try and improve the privacy protections here.

Thank you very much for your indulgence.

CANADY: Thank you, Mr. Davidson.

Mr. Perrine?

PERRINE: Mr. Chairman and members of the subcommittee, thank you for inviting me to testify on the subject of **Carnivore** and the Fourth Amendment. I believe that the current debate over the **FBI's** new digital wiretap tool commonly known as **Carnivore** is really about the risks in attempting to simply translate the policies, law and practices of telephone wiretaps to the digital realm of the Internet.

Today's testimony has shown over and over again that there are -- that these differing interpretations of old law, as applied to the Internet, may be leading to problems.

The debate should not be about this specific program. The real issue is how the government is attempting to extend its lawful access to the Internet. In the process of applying old laws to the new media, the

privacy of citizens may be eroded in ways not intended or permitted under current wiretap laws.

In my career in computer security, I've always been an advocate of personal privacy, unrestricted access to strong encryption and less government oversight and intervention in the lives of law-abiding citizens. Due to my work at the Super Computer Center, I also understand the need of law enforcement to be able to intercept traffic. We spend an awful lot of time detecting, analyzing and tracing computer intrusions.

But this is about balance. The needs of law enforcement and privacy are not mutually exclusive. There can be a balance between them.

Earlier this year, while I was visiting the **FBI** to discuss critical infrastructure vulnerabilities, I was invited to see **Carnivore**, although we didn't know it by that name. In technical terms, **Carnivore** is a high-speed packet sniffer with very aggressive filtering capabilities. It does examine all of the data packets passing through a network and filters out the data that does not meet its filtering criteria. This is very similar to tools that are already available in private hands. Every network administrator uses a packet sniffer in diagnosing problems. **Carnivore** has new functions in the way that it can aggressively filter and perhaps in the speed of the networks that it can monitor.

Carnivore does not appear to be a monitoring infrastructure -- and someone did use the word Echelon -- capable of real-time monitoring of large numbers of phone calls. It does appear, on its face, to be a tool specifically designed to meet the rigid requirements of a Title III wiretap order or pen-register order.

Recent news stories have compared **Carnivore** to a trunk-side wiretap, which is monitoring system that allows monitoring all communications running through a phone office, just to find the calls related to a suspect. Congress rejected the use of trunk-side wiretaps more than 30 years ago because they mix communications of the innocent with those of suspects. This is an interesting comparison, but may be flawed. **Carnivore** does at a fundamental level intercept and examine all Internet traffic, but it only does that in order to select or reject data based on its filtering rules.

The question comes down to at what point has an examination and the privacy violation actually occurred? Does the examination and the privacy violation occur if a program compares the intercepted data with its filter and then rejects the data, or does the examination not truly occur until the data's seen by a human being or if this is stored for later processing?

This also comes into play -- this trying to use an analogy of the old telephonic system into the Internet -- we've talked a lot today about pen registers, which the purpose is to require -- to acquire the phone numbers used. And we've also heard testimony that that is functionally equivalent to the to and from e-mail addresses. Are they the same? Actually, I think not.

But **Carnivore** is just a tool and its capabilities must be considered in the context of how it could be used. **Carnivore**, with no filters, appears to be capable of gathering all of the information passing through the network that it monitors. There's nothing to stop a person from **Carnivore** technically -- using **Carnivore** to monitor all the network traffic passing through an Internet service provider if they had the capacity. There's no way for anyone to know the configuration of the filters in a **Carnivore** system at the time that it's installed or the true capabilities of **Carnivore** without examining the source code of the system during installation and the filters during the monitoring process.

The ACLU and others have called for publication of the course code of the **Carnivore** system and their arguments are compelling.

PERRINE: However, a one-time publication or review of the source code, even by an independent verification validation organization, would provide only a snapshot of **Carnivore's** capabilities, with no assurances that the **Carnivore** program actually installed on an ISP was built from the sources that was reviewed.

Carnivore is also under constant development, so the source code snapshot that was reviewed would be out of date within a few weeks. So unless you're planning on having an ongoing independent verification validation process, you'll never know that what was installed was actually what was reviewed. And there is no source code review that would indicate the filters that were installed in **Carnivore** at a given ISP on a given case.

So, in conclusion, **Carnivore** does appear to be both a trunk-side wiretap and an attempt to bring limited wiretap capabilities to the Internet. It does have long-term implications for privacy that must be carefully considered. Old laws often breakdown when applied to the Internet, and I think we've seen that today. And applying these old laws, may unintentionally erode constitutional protections in unintended ways.

Law enforcement may need appropriate legal access to Internet communications under limited circumstances, but this access must be properly controlled and monitored to ensure that constitutional safeguards are maintained.

Thank you.

CANADY: Thank you.

Mr. Corn-Revere?

CORN-REVERE: Chairman Canady and members of the committee, thank you for inviting me back to testify on this important topic.

Rather than try to paraphrase my written submission in five minutes or so, I'll dispense with that and just try to address some of the points about **Carnivore** that were discussed in the testimony of the government witnesses. I'll just try and touch on two or three points related to what, in my experience, was **Carnivore** in its natural habitat.

One of the first points that was made is that **Carnivore** is used in only very limited ways; that it's used only when an Internet service provider either cannot or will not comply with a court order.

In fact, Mr. Painter testified that in the one challenge that he's aware of, that incoming e-mail addresses, but not outgoing e-mail addresses were received, that then required the government to move forward with the installation of **Carnivore.** That's not quite what happened in that case.

In the case in which I was involved, the ISP did try to comply with a lawful court order, the pen-register and trap-and-trace order. It's simply taken as a given, the ISPs are obligated, under the terms of the Electronic Communication Privacy Act, to comply with lawful orders of the -- lawful court orders to provide information, but at the same time, they're required to protect the privacy of their subscribers.

In this case, the solution that the ISP put in place did get all of the outgoing -- excuse me -- all of the incoming e-mail addresses, and it did supply a smaller number of outgoing e-mail addresses to the government. They were dissatisfied with that, saying there must have been more outgoing e-mail addresses.

In fact, we tried to explain, that they're any number of reasons why there may be fewer outgoing e-mails, then there were incoming e- mails. For example, the target of the investigation might have used a web-based e-mail source, rather than using his own resident program. But nonetheless, the U.S. marshals were dissatisfied with that solution and informed the ISP that they were coming to install **Carnivore** within two days. That's what prompted the court action that led to the magistrate's order.

I believe, Mr. Painter then testified that, since that time the ISP has provided excellent cooperation.

In fact, the ISP has done in subsequent cases what it did in that case. It provided and offered to provide ways to comply with orders that it received in ways short of installing **Carnivore**, and since that time **Carnivore** has not been reinstalled on its system.

Secondly, in response to a question from the chairman, one of the government witnesses suggested that it was the ISP and its implementation and not the **Carnivore** program itself that caused a crash and disrupted the ISP's system.

In fact, our experience was that **Carnivore** was incompatible with this system, requiring the ISP to make adjustments which led to a number of problems, that ultimately led to **Carnivore** being taken out, and then the next day the order for its installation expiring.

Let me say just one other thing about that order. In fact, there was a magistrate's order, still under seal, that did require the installation of **Carnivore.**

CORN-REVERE: We tried to work out in the terms of that order what safeguards we could to make sure that no more information could be collected than necessary. But, in fact, what the magistrate said in that order was that he would welcome the decision on the legality of **Carnivore** under the existing legal scheme to be decided by a reviewing court. We haven't had that kind of legal review yet, and I don't know of a case in which that may occur.

Next, the government witness talked about the number of safeguards that exist to make sure that **Carnivore** does not lead to excessive violations of subscriber privacy. For example, Dr. Kerr testified that the filter will ensure that **Carnivore** acquires only the information that is authorized by a court order and suggested that it would be necessary to obtain the assistance of a technician or even perhaps the assistance of the ISP to alter the programming of **Carnivore** so that a rogue agent might gain information to which he or she is not entitled.

I'm not a technician, so I can't really address that point, but I can say that in the case that I was involved in, I was told that **Carnivore** would be accessible remotely by government agents and that the configuration of **Carnivore** could be changed with the flip of a switch. Maybe that's correct, maybe it's incorrect, I don't know. It does suggest, perhaps, that the proposals that have been discussed earlier for independent review of **Carnivore** really are in order.

Next, we're told that we will be protected from invasions of privacy because there is an audit trail that makes sure that the filter is correctly set to correspond to what is authorized by the court order and that that will be available with the evidence in a prosecution. But in fact that's a safeguard that exists only if there is a prosecution, and the safeguards that exist under the law primarily exist for Title III interception orders, not for trap-and- trace orders.

There is no requirement to notify the target of a surveillance in a trap-and-trace situation that that surveillance took place. So if -- there's no way to ensure accountability in that circumstances.

As I had mentioned in my April 6 testimony, surveillance was undertaken briefly with **Carnivore** pursuant to a trap-and-trace authorization, which, as many people have noted here today, is available only with a showing of relevance -- certification of relevance by a law enforcement authority; there is no requirement of probable cause necessary.

I believe Congressman Bachus asked whether or not **Carnivore** has been used for violations of any other laws, such as antitrust laws or consumer protection laws or anything else. The response was given that **Carnivore** can only be used in the event that there are specified federal felonies as set out in Title III.

As a matter of fact, that's true only for Title III intercept orders. You're not required -- or you're not limited in the use of **Carnivore**, in the event that it's being implemented in response to a trap-and-trace order, to the felonies that are specified in Title III. All that has to be shown is a certification that the prosecutor or the law enforcement agent involved believes that the use of **Carnivore** would be relevant and the information gained would be relevant to an ongoing criminal investigation.

The rest of what I have to say is really just paraphrasing what I've written down and that's already submitted. And I'll just leave it at that and be happy to answer your questions later.

CANADY: Thank you, Mr. Corn-Revere.

Mr. Blaze?

BLAZE: Thank you, Mr. Chairman.

I should point out that my comments here don't necessarily represent the viewpoint of my employer. I'm here, so to speak, on my lunch hour to provide the scientific and technical perspective.

My interest in the problem of intercepting traffic on the Internet for analysis dates back to my doctoral work, where I built a system to collect traffic that I would analyze as part of my dissertation work. What I discovered then, and what's certainly become even more the case as we've gone to higher speed and more complex kinds of networks with more protocols running on top of them, is that the problem of collecting data from Internet packets, from the packet level, is a very subtle and difficult one.

BLAZE: So my comments today address the question not of how do we ensure against the possibility of malice or misdeeds on the part of law enforcement, but starting from the premise that everybody is acting with good will and honest -- and perfectly honestly, even still it's difficult to be sure that the tools being

used to collect information from packets, in the way Carnivore does, are behaving faithfully and reliably.

In particular, there is a strong possibility that omissions of collected data or garbling of collected data could cause misleading results that could put information collected out of context, or collect data inadvertently that should be attributed to another source or destination than it may initially appear.

There is no systematic way, unfortunately -- we in the computer security community learned this over and over again, these are hard- won lessons -- there's no systematic way to deal with large complex systems of software, particularly when the function of the software is security-critical. Certainly, Carnivore is a security-critical function.

One of the particular difficulties of managing complex secure systems is that very often they fail silently. They fail in a way that leads the observer to believe that they're working properly, but, in fact, subtle bugs mean that there are vulnerabilities or mistakes there anyway.

So we have the problem of being concerned with the reliability of data collected by a complex piece of analysis software, and the problem of ensuring that something connected deep within the infrastructure of an Internet service provider isn't itself vulnerable to external tampering or could itself be -- have control taken over by a malicious third party who is able to get access to it by exploiting some bug.

There're two ways that we stumble along in trying to assure ourselves that complex systems that we want to rely on are. in fact. trustworthy. One is by focused review by experts by audits, and I certainly want to strongly advocate that the kind of focused review by independent experts that was discussed in the first panel be done. But there are limits to what a limited set of experts can ever discover. We discover again and again that even after a security audit, new information comes out about the environment in which the software may be used or something may have been missed by the panel of experts that could only be known by widespread publication of the source code and details of the architecture of the system.

The security community, pretty much unanimously, supports the idea that source code should be published for any system that performs a vital security critical function. And I think the Carnivore system is a very good example of this.

Now, one of the objections raised to doing this in the case of Carnivore is that it might provide aid and comfort to the targets of investigations, who might find ways to circumvent the system. I think, in the case of Carnivore, the existence -- the mere existence and the architectural details of the Carnivore system don't really provide much help to the -- to someone who wants to evade it. It's very much like knowing the details of how a tape recorder works doesn't help you know that there's actually a microphone that's been installed in your apartment.

Instead the important information that a criminal would be interested in are the details of whether or not Carnivore has been installed in a particular place.

BLAZE: And, of course, no one advocates publishing the details -- the operational details of specific Carnivore installations.

So, in summary, I recommend that we -- that neither -- that while neither focused review by independent experts nor publication of source code are panaceas and ensure against any possible problem or abuse,

these are essential steps -- widely recognized essential steps that certainly should be done in this case. And I hope that will happen.

Thank you.

CANADY: Thank you, Mr. Blaze.

Mr. Baker?

BAKER: I've been on both sides of some of these debates. And I have to say I see both sides of this one. I think in some ways, both sides of this debate are stuck in a -- in the telephone world. A lot of the witnesses, some of the questions, suggest that maybe we could solve this problem by having ISPs take responsibility for doing these intercepts themselves.

And actually I think the FBI has got this about right. If the ISP wants to do it, then they should do it. But if you take an ISP -- a small ISP, and tell them, "You have to do it," they're going to treat this like an expensive unfunded mandate. And there's no reason why they're going to do it more enthusiastically or more privacy- protectively than the FBI. In fact, there's going to be less oversight.

This is not the phone company that could just hire somebody to do the wiretaps every day and add it to the rate base. They're not going to be doing what people saw the phone companies do by way of protection if they're small ISPs and they don't want to have this role. And I'll tell you there's plenty of ISPs that really don't want this role in spite of the noisier ones who do.

But I think the FBI and the Justice Department are also living in the past. To say you don't have an expectation of privacy in information that is in the hands of a third party in the Internet age is just crazy. I mean, our entire lives are in the hands of third parties.

To treat the to and from lines in e-mails as though they were just the same as the phone numbers that you dial is also bizarre. We know that the phone company collects those phone numbers because they send us a bill with those phone numbers every month. No one expects the ISP to be collecting our to and from lines, especially not the from line. They don't use the from line to deliver the message, you know. That's just content, and they should get a Title III order to collect it.

So if relying on the ISP doesn't work; if this really is a privacy problem, what should we be doing?

I guess I would say a couple of things. First, as Mr. Nadler suggested, we ought to be sending notice to people when they've been subjected to this kind of intrusion. We have a system right now that protects the privacy of the crooks, but not the innocent people who are investigated.

You know, if Mr. Davidson were under investigation -- he sent that e-mail to Mr. Taylor. The next step that the police would take would be to put a cover on all of Mr. Taylor's e-mails in and out. It's perfectly relevant to their investigation. They want to know whether he's also corresponding with other crooks that they're investigating. So they're going to have 60 days or 120 days of Mr. Taylor's in and out e-mail, just automatically. And he'll never know it, because he's not going to get indicted and get to see that information.

There ought to be notice. Only you guys can make that happen.

There ought to be oversight. The audit provisions, again, are very protective of crooks, but not of innocent people. The criminal defense attorneys are going to get to see this and they're going to be able to follow that audit trail, but Mr. Taylor, if his e-mail has been intercepted, isn't going to get a chance to see that audit. There needs to be somebody who will do that audit on behalf of ordinary citizens; we shouldn't be relying on criminal defense attornies to do that for us.

Last point, if you want to do something about this, you probably ought to do it pretty quickly. That's because **Carnivore's** not the only way in which this is going to happen. The Communication Assistance of Law Enforcement Act had a provision that said, well, everybody has to provide trap-and trace-capability. The **FBI** has said that means packet data carried by carriers has to have a trap-and- trace capability. The FCC has said, We're telling everybody, you've got to have something installed -- all you carriers have to have the capability of doing this trap-and-trace by September of 2001.

BAKER: We aren't going to tell you how to do it, but we're going to tell you you have to have it done by then.

There's only one -- well, there's two ways to do it: either let the **FBI** install **Carnivore** or you go out buy **Carnivore** on your own. I'm not sure those are really the only solutions that we want to have carriers have, but unless the FCC backs off of its deadline and its current mandate, that's what's going to happen and it'll be too late to install a lot of controls.

Thank you.

CANADY: Thank you, Mr. Baker.

And last, but not least, Mr. Sachs, and I apologize for not having more table for you there.

SACHS: That's OK. I'm going to be very brief in the interest of time.

My name is Peter Sachs, and I'm the president of ICONN. We're a small Internet service provider based in New Haven, Connecticut. And I believe I'm one of the small ISP that Mr. Baker may be referring to.

We do have the capability -- in fact, any ISP has the capability of supplying the **FBI** with exactly what it wants in a more accurate, more efficient and more private manner, because we have absolutely no need to look at anybody's information, except for the actual target.

FRANK: Mr. Chairman, could the witness speak up a little more, please?

SACHS: Any ISP can do this, in as little as two lines of programming code. It doesn't require any machine. It doesn't require any specialized programming skills, beyond the programming skills of a normal system engineer at an Internet service provider.

To confirm this statement, I asked my system engineer to set up a system to monitor all of my communications. And in less than hour he was able to see everything that was sent to me or from me on his machine in clear legible text. So there's no need for any specialized machine or any, sort of, specialized knowledge to be able to do this.

Carnivore also creates an extreme security risk for an ISP. To allow a third party to attach a computer, especially a secretive computer that's accessible from a remote location, to an Internet service provider is unheard of. It just provides any hacker out there with yet one other doorway into which they can enter your network, and essentially destroy your network along with all of the data of all of your customers.

Carnivore also presents a performance hit for an ISP. The moment you intercept all information flowing over an ISP's network, which is what **Carnivore** does, it causes a bottleneck. Bottlenecks cause slowdowns. As all of you know, the Internet is already slow as it is; slowing it down even further, doesn't help matters much.

Lastly, it may have a chilling effect on the information that my subscribers or any ISP subscriber sends over the Internet. If you're not going to send something because your afraid of its content or perhaps just its destination, it raises very valid First Amendment concerns.

If the ISP gathers the data for the **FBI** under a court order, the **FBI** can't possibly see anything it's not supposed to see, because they're only getting what we give to them. If the **FBI** does the work, they at least have the ability to see anything they want, and they do, in fact, have the ability to see anything they want. The former method protects privacy and the latter method invites abuse.

Since the ISP can provide the ISP with exactly what it wants, without imposing upon the privacy rights of all the subscribers, why **Carnivore**? Why use the most intrusive means if the least intrusive means are readily available?

Thank you.

CANADY: Well, I want to thank all the members of this panel for your very helpful testimony.

I just have one question, related to Mr. Sachs' testimony. Mr. Sachs has testified that doing the interceptions or executing a trap- and-trace or pen-register order is a simple matter for any ISP; can be done in an hour, just a little programming and there it is. Now, that's not consistent with what the **FBI** has told us their understanding is.

And let me ask -- I guess maybe Mr. Blaze and Mr. Perrine would be two who might be in the best position to give me your take on whether it's closer to what Mr. Sachs says or exactly as Mr. Sachs says or what the **FBI** has had to say on that.

Is it as simple as -- and I'm not trying to be -- single out Mr. Sachs here, but that's a fundamental question for us to look at. Is it as simple from -- in your understanding as Mr. Sachs has presented it, or does he have a programmer that has special expertise that other ISPs might not have?

PERRINE: Well, I can address that from the standpoint of tracing computer intrusions and attempted

intrusions, I would say probably 30 to 50 percent of the ISPs that we contact don't keep much in the way of logs. We tend to deal with a lot of the smaller ISPs, we tend to see the same ISPs -- the problematic ISPs over and over again.

I think that it's fair to say that many ISPs could solve this problem if they were motivated to, but it's not a profit center. They aren't making money cleaning up or preventing computer intrusions at other facilities and they certainly aren't going to make any money providing information to the government.

PERRINE: They're not financially motivated to do it. Some of them have the technical capabilities, and I would have to say that there are some of them that do not.

CANADY: Mr. Blaze?

BLAZE: Sir, I'd just like to -- from a technical perspective, the answer is like most subtle, technical questions, It depends.

The problem with a system like **Carnivore**, from the point of view of complexity, is that it has to be general purpose; it has to work under a wide variety of operational conditions; and it has to work to collect a wide range of kinds of information, depending on what the court order is asking for.

Some ISPs may already have in their network, for example, logs of information. They may have, for example, port replication capabilities on switches that allow them, much more conveniently than an external tool, to collect the kind of data that **Carnivore** or a **Carnivore**-like system could only collect with some trouble and with some difficulty assuring yourself that it's operating correctly.

In other cases, there may not be the exact capability required, so, it depends.

PERRINE: If I could just add -- if the equivalent of **Carnivore** were available in open source, that would make the -- that would lower the barriers to entry for the smaller and less technically capable ISPs to provide this information.

And I think that this is something that is quite feasible. It's not a six-day project, it's not a six-year project, it's probably on the order of I think maybe three to nine months at the outside for the open source community to reproduce large parts of the **Carnivore** system. And that would make it easier for smaller ISPs to provide this information themselves.

DAVIDSON: Could I just jump...

CANADY: Mr. Davidson, sure.

DAVIDSON; Perhaps part of the problem in coming up with an answer is that we don't know exactly what **Carnivore** is doing. There seems to be a certain subtlety of analysis that the **FBI** is seeking. And perhaps the **FBI's** interpretation of what numbers dialed on a telephone is, in terms of extrapolating it to the Internet, might be different from what many of us would think it would be.

So we really -- it's hard to answer the question about whether ISPs can do what **Carnivore** does until we, sort of, know what **Carnivore** does.

CANADY: Well, I understand that. But I also understand the **FBI's** problem with making the source code publicly available if there are proprietary interests there. I mean, there are other people's rights that have to be taken into account if they've used proprietary information in developing that. So that's -- I don't know how you resolve that. It may be that you just develop another product that could be used in the way that Mr. Perrine described it.

I want to conclude my time by thanking all of you for your contributions. They have been very interesting. And I would -- I will also ask that you be open to receiving questions from the committee and responding in writing, if the committee sends you questions. That might help us as we complete the development of the record for the hearing. But we thank you very much.

And I recognize the gentleman from North Carolina, Mr. Watt.

WATT: Thank you, Mr. Chairman.

And in the interests of time, I'll try to be very brief, too. I've got two technical questions also.

Mr. Perrine mentioned the possibility of doing something similar to **Carnivore** on an open source basis. Am I mistaken that that would create a different set of problems? Wouldn't that, in effect, make the technology available to everybody? And you're not suggesting I walk in to Radio Shack and buy me a **Carnivore** system so I could tap into everybody's Internet?

PERRINE: Well, actually, I almost am. It turns out that **Carnivore** appears to be functionally similar to network sniffers that are actually shipped with commercial operating systems and free operating systems today. The special purpose -- or the special magic for **Carnivore** appears to be that it is capable of filtering out information in ways that other people haven't had an incentive to write a program to do it, and also that it can monitor higher speed networks. And I believe that that's probably where a large part of the proprietary code is is in the very high speed monitoring.

PERRINE: And I believe that that's probably where a large part of the proprietary code is, is in the very high-speed monitoring.

But, as other people have mentioned, the idea is to neck all of the large pipes down to small pipes and then monitor those. And if the ISP can do that, then they don't need the ultra-high-speed monitoring capabilities.

And I think Matt has...

BLAZE: Yes. I addressed some of this in my written testimony. But the important point is that there's nothing sinister about the basic functionality of network sniffers. They're an essential tool, used by anyone who has to administer a network, such as an ISP or a local area network administrator. These tools are common place; they're widely available.

They may not have the -- they don't have the requirements for keeping the kinds of legal audit trails that a system like **Carnivore** would have. So the additional capabilities that something like **Carnivore** has don't provide additional interception capabilities, but rather provide these legal assurances and chains of evidence and audit trails that open source would benefit greatly from and that wouldn't provide any great aid to bad guys.

WATT: Mr. Baker, it looks like you...

BAKER: I have to say I think the **FBI** is right on this. If you publish exactly how you're filtering this, then people will try to write their e-mail addresses and spoof their e-mail addresses in ways to avoid that particular method.

It's really not the best idea to publish this. I think the likelihood that the public's -- the open source community is going to embrace **Carnivore** as a project is about zero. There are going to be very few benefits from doing that and a lot of costs.

WATT: Mr. Corn-Revere raised an issue that I want to not have him address because he's already acknowledged that he doesn't have the technical capacity to address it, but Mr. Blaze and Mr. Perrine and Mr. Davidson, maybe Mr. Sachs, Mr. Corn-Revere raised the prospect that Carnivore could be accessible remotely.

I think I understand what that means, that you could -- the **FBI** could sit in an office somewhere else and change the program and manipulate it from some remote location. That's what you intended, Mr. Corn-Revere?

CORN-REVERE: That's correct.

WATT: OK. Tell us whether that is technically feasible, since Mr. Corn-Revere doesn't know the answer to that, give me -- my technical experts can tell us...

PERRINE: Actually, I believe that is the case.

WATT: It can be remotely...

PERRINE: I believe that is the case. I had a very limited time to see it, but I believe that is true.

WATT: Mr. Blaze?

BLAZE: I should point out that the ability and necessity to be remotely controllable and configurable is precisely what we, in the computer security community, are made very nervous by. That capability potentially, if not implemented very, very carefully, could allow an external attacker -- third party -- to gain control of the system and potentially do quite a bit of damage.

WATT: Mr. Davidson, Mr. Sachs, if you'll address that same question quickly, I'll leave everybody else

alone.

SACHS: Sure. The remote accessibility is almost as bad as the invasion of privacy. Given the record of hacking of government web sites, which happens almost on a weekly basis, the fact that this secure **Carnivore** machine is going to be out there accessible remotely means any hacker can get into a system.

If they could get into the White House and hack that site, they can get into an ISP through **Carnivore**.

DAVIDSON: Changing the configurations remotely to the extent that it's possible, I mean, I think removes part of the check that we would hopefully think exists where an ISP at least is in some ways an intermediary of how the device is deployed. And so that raises another concern.

WATT: Thank you, Mr. Chairman.

CANADY: The gentleman's time has expired.

The gentleman from Alabama is recognized for five minutes.

BACHUS: Thank you.

Is there any rationale that any of you can think of why electronic mail or information traveling over the Internet should have less protection than, say, a person's telephone calls or their faxes or either their private mail?

SACHS: No. To the contrary, I think that in fact it should have at least as great a protection as we currently give to voice communications for example in Title III. There's a crying need, really, for the Congress to update the Electronic Communications Privacy Act to bring it into line with the expectation of privacy that I think that Mr. Nadler suggested and that most of us have.

These are, in many respects, our most important communications, involves our most sensitive data and our most private thoughts. And we do need to bring those into line.

The administration -- if I can for just a second -- the administration, I think partly in response to the **Carnivore** controversy, made some suggestions the other day. Mr. Podesta made some proposals. In my testimony, I've gone through those proposals in some detail. When you get a moment, I urge you to take a look at that.

But I want to stress this one point: Those proposals are not a solution to the **Carnivore** problem. Tweaking the surveillance laws, the wiretapping laws, doesn't get to the heart of the **Carnivore** problem, which is that it is a device that does allow the **FBI** to filter through, potentially to capture, huge volumes of communications, most of which are completely unrelated to the target of the investigation.

That's the real problem with **Carnivore** that the committee needs to address; Congress needs to address, I think by telling the **FBI** clearly, if it's not already clear in the statutes, that it doesn't have the authority to force a service provider to install a device like **Carnivore**.

BACHUS: Mr. Davidson?

DAVIDSON: In the interest of time, I'd just like to say, ditto. And add one point, which is that e-mail is really just the tip of the iceberg here.

I think that was part of the point I was trying to make is that the home has explored; things that we used to keep in our possession are now making their way out onto a network. And this is a trend that's only going to increase: finance records, health records, stock portfolios, information about your kids, all being stored somewhere else. Once it leaves your possession, the kind of protection is has under the law is greatly diminished. I think that's really the challenge here for this Congress, to think about how we deal with that.

BACHUS: I think Justice Brandeis predicted about 40 years ago that one day the government would be able to come into your home and basically determine everything you did and said. And I think maybe that day's arrived.

Anyone else wish to comment on that?

I read a question to the first panel which was that you can't go to the AT&T and say, We're going to analyze all the phone calls that go through your system. I mean, that's true, right? Can't do that. But isn't that what they're doing with ISP providers?

STEINHARDT: I think that's exactly what they're doing with an ISP provider. And it's not so much a technical issue, it's a legal issue. I think the **FBI** and law enforcement accepts it could not go to a telephone provider and install a **Carnivore**-like device, the kind that Mr. Perrine referred to. He said that was settled 30 years ago, and he's quite correct.

I think that the -- I think the legal basis for doing that to an Internet service provider is at least equally suspect, but it may take an act of Congress to clarify that point.

BACHUS: I think clearly the marketplace and technology has outrun the law, and in doing so has overrun our legal protections that have been in the law for years.

Let me ask you this: In your experiences, what procedures are typically followed to notify customers when information from Internet service providers and other companies about them is subpoenaed or requested by the government? Is there any notice?

BAKER: That's a very mixed bag. And it depends entirely on the policy of the ISP. Some ISPs have a policy of sending notice, others do not. There's no requirement one way or the other.

It seems to me that notice is a good idea. The government probably should be sending it, rather than relying on ISPs to say yes or no to notice.

BACHUS: It's my understanding that what they're saying is they don't have to give notice if there's a

reasonable expectation that if they gave notice the communications would stop. And I think in every case where they gave notice, it would be a reasonable expectation that the communications would stop, so.

DAVIDSON: You know, in some circumstances, we have delayed notice, and I think that that serves a very important purpose here, too. And I think there'll be circumstances where that's appropriate. At least then you know that this had happened, you have a chance to object to it, even if it's after the fact.

CANADY: The gentleman's time has expired.

The gentleman from Michigan, Mr. Conyers, is recognized.

CONYERS: Well, I begin by thanking this second panel, because this has served as a very important corrective for what we were just told for a couple hours earlier. And I'm sorry to hear that we ought to move very rapidly on this matter because the clock is running down on the 106th Congress. There's not much likelihood of that. But I'm hoping that this will prepare us for a much deeper investigation that we're going to have to indulge in.

Let me thank specifically, though, the American Civil Liberties Union, because they, in addition to this complex subject, work on a number of others that appear before the Judiciary Committee. And so I'm glad to see them working here as well.

Is there a feeling that we should probably try to require that notice be given to those who are the objects of a trap-and-trace measure, or is that getting a little bit too fine -- cutting too fine a line in the requirements on the Department of Justice?

Mr. Corn-Revere?

CORN-REVERE: Well, let me just address that question in the context of the previous one, and that is, in the case of an ongoing investigation, like with the trap-and-trace order, the ISP is expressly prohibited from providing notice. Otherwise if the target of the investigation knows that he or she is being investigated, then the communications will cease. So there's no notice before the fact.

I think it would be advisable at least to change the law so that anyone's who's been the target of a surveillance be notified after the fact, as currently is the case with respect to a Title III intercept order.

DAVIDSON: I would just add that I actually think that there are two more important things for trap-and-trace and pen registers, one of which is raising the standard which is extremely low right now for access to this information. The second is defining what trap-and- trace and pen register mean for the Internet.

As you see -- I mean, there's been this wild extrapolation of numbers dialed into somehow this, sort of, much more meaningful origin and destination of Internet communications. And I think that needs to be dealt with.

CORN-REVERE: If I -- if I could just add to that point, because Mr. DiGregory did cite the Supreme Court decisions finding that pen registers don't violate the Fourth Amendment if there's no warrant, because there's no reasonable expectation of privacy on that information.

If you actually go to those Supreme Court opinions -- and there are really two of them that address it, Smith vs. Maryland and United States vs. New York Telephone Company, it's important to read what the Court had in mind when it said that no privacy right was being invaded.

For example, in New York Telephone Company, the court said that a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed, a means of establishing communication. Neither the report of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed, is disclosed by pen registers.

Now obviously, that's very different from the kind of information that's acquired with respect to e-mail. Anyone who gets my e-mail address knows the identity of this party. It has my name in it. And that's true of many other people with e-mail. Certainly, if you're able to get URLs -- uniform resource locators -- for browsing on the Internet, that's the same as getting somebody's library record or the record of videotapes they have checked out.

CORN-REVERE: So, the kinds of information available on the Internet is completely different from what existed in the context of a pen register when the Supreme Court addressed those issues some 25 years ago.

STEINHARDT: If I could just add to that, first, Mr. Conyers, thank you for your price for the ACLU, I'll except that on behalf of the organization.

There's one other thing that I think the Congress needs to attend to, and that's the standard now for law enforcement to get access to stored records, which is extremely very low.

But as Mr. Nadler point out, people who expectations of privacy don't diminish by the fact that an Internet service provider may have, for an instant or perhaps a little longer, been holding those stored records. And we need to begin to treat those as the kinds of records which the FBI and other law enforcement agencies need probable cause in order to obtain.

CONYERS: Well, gentlemen, I see this attempt to bring into balance the tensions between the Department of Justice and the Constitution -- citizens' rights to be an enormous one. I see a complex, I see a changing, because, as new technology comes on -- are there any of you here that can give me any words of assurance that it may not be as big as it seems to be this afternoon? We probably need some...

(CROSSTALK)

CANADY: The gentleman's time has expired.

And the gentleman from Arkansas will be recognized.

HUTCHINSON: Thank you, Mr. Chairman.

And I was absent during some of this testimony, but I want to assure everyone that I've read your testimony and have a great interest in your viewpoint on it. And I think everybody here probably was present during the previous panel's testimony, and I'd just like to ask a general question to Mr. Davidson, perhaps Mr. Steinhardt.

Did both of you hear the testimony of the previous panel? I'd just like to ask a reaction as to -- I mean, from what I gathered from the first panel's testimony is that, first of all, everything through to the **Carnivore** program is proceeded by a court order.

The -- secondly, a concern is whether there should be some independent review of the source codes. And I think that's something I had a discussion with them on -- you know, they're submitting it to -- willing to spend an independent evaluation, I think there's a question whether there should be some type of ongoing review, but I think that's an issue that's out there.

And then, you know -- but I was asking questions that -- you know, they're retrieving information for the **Carnivore** program, not for purposes of expanding what they achieved -- or received, but to limit it and to minimize it. And so, if you could just comment on whether you disagree on any of those conclusions?

Mr. Davidson?

DAVIDSON: Let me start by saying, I think some of those things actually sound good. And I mean, I think the idea of trying to minimize information that's collected in a context of an Internet, you know, surveillance is a good thing.

I think the problem is we just don't -- A, we don't know, really we don't know how well it's going to be doing that. And we've got to have a chance to look under the hood and understand this. And I think courts are going to need an understanding and defendants are going to need to understand it, and people are going -- public needs to build some confidence in it.

HUTCHINSON: And how would you suggest doing that?

DAVIDSON: I think this notion of opening up the code, I think is a very good one. If there needs to be a preliminary step of getting an independent panel in here, that's not the same and it wouldn't be as good as opening it up to the public.

I think that -- personally, I think that any system that relies on -- if I can be so easily violated by somebody knowing how it works, then I don't think it can be that useful a system. If the bad guys can figure out, you know, how to evade it that easily, then, you know, how good can it be? And I think that -- I'm not convinced yet that opening it up is a bad idea. But maybe that's what we can get an independent group in here for.

I think, but, you know, from a greater point of view, there's, sort of, this -- the issue it raises is, there is this desire on the part, I think of law enforcement to be able to extrapolate every current capability, like pen registers or trap-and-trace orders, into the Internet world. The fact is, that when you do that, some of them don't translate very well.

Pen registers is probably the example we've talked about the most here. When you -- we don't know what

they mean in the Internet world when we try to extrapolate them, we get a lot more information...

(CROSSTALK)

HUTCHINSON: You suggest a higher standard for a pen register for Internet access?

DAVIDSON: Absolutely a higher standard and a clearer definition of what it means. But I think there's got to be an understanding that some things they're going to be able to do -- I mean, there are new capabilities that the **FBI** is getting all the time, because of the sea of information that's out there.

The Internet's a very good thing on some level for law enforcement. I think there's going to have to be a recognition that maybe some of the things they can do now they'll have to do differently in the future. It's not necessarily a horrible thing. There's going to be lots of new tools for law enforcement as well.

HUTCHINSON: Mr. Steinhardt?

STEINHARDT: Well, in my mind, the testimony from the government panel raised more questions than it answered. I mean, for example, the testimony, it seemed to me to suggest that the only thing that **Carnivore** is, at least at the moment, and I think the implication was to be primarily used was the interception of e-mail.

STEINHARDT: But we know from -- I know from those persons who have seen some of those demonstrations, for example, members of the press who have seen some of these demonstrations of **Carnivore,** that it is capable of analyzing and potentially intercepting far more than just e-mail. There are a whole range of Internet protocols which **Carnivore** is capable of filtering for. There was some allusion to those here today.

HUTCHINSON: Could I interrupt you here for a second?

STEINHARDT: Yes.

HUTCHINSON: I mean the government has that capability of doing unauthorized wiretaps. They have the capability of gathering more information than they're entitled to under a court order. It's the court order that restrains the use of gathering techniques. And so there's always consequences to that.

But I mean obviously any of these can be abused, and they could gather more information but they're limited by a court order.

STEINHARDT: No, no, perhaps I wasn't clear Congressman Hutchinson.

CANADY: I'm sorry, the gentleman -- if he could finish in 15 seconds, because we're -- we need to conclude. The gentleman's time has expired.

STEINHARDT: Well, the government witness, for example, suggested that they had one case -- had gotten files through the file transfer protocol. The committee didn't have an opportunity to get into that question, but I think there are serious question about whether or not existing law permits them to get that for example with a trap-and- trace order.

HUTCHINSON: Thank you.

CANADY: The gentleman's time has expired.

The gentleman from New York, Mr. Nadler, is recognized for five minutes.

NADLER: Thank you Mr. Chairman.

I have a series of questions. I hope the answers will be brief because of the time limitation.

Someone said before that the **Carnivore** system is kind of sniffer system, that there are many others out there. So, you could have a lot of private sniffers. How do you -- how would we -- if there a danger that private sniffers can get all sorts of information violating people's privacy and how would we know that it has happened?

BLAZE: Someone who wanted to use a commonly available sniffer program to violate some one's privacy, would still have the problem of getting access to the network over which that traffic flows. That's the hard part, getting the software to do the interception.

NADLER: That's what the **FBI** is asking us to let -- to mandate the ISPs to do in this case?

BLAZE: Right.

NADLER: OK. Thank you.

Secondly, we talked about the question of remote accessibility of the **FBI -- of the Carnivore** system. And someone mentioned that you could change the configurations remotely. Do I understand correctly that what is saying is that the **FBI,** or for that matter a hacker, could, by changing the configurations, could, in effect, change evidence and implicate somebody in some crime if they had a motivation to do that?

BLAZE: Well, the answer to that depends on the security of the remote access system. If its implemented in a secure manner, then the chances of that are very small. If it's implemented in an insecure manner, then the chances of that become quite great...

NADLER: Let's assume, let's assume that the police were under some -- we know that this has happened in the past -- the police were under some great pressure to solve some heinous crime and they figure they've got their guy and let's just give a little more evidence. Could they use the **Carnivore** system to, in effect, manufacture evidence?

BLAZE: That would depend on how the audits are implemented and that's one of the reasons that open review would be a very useful thing.

NADLER: So, the answer is yes, unless you put in safeguards to prevent it?

BLAZE: Yes, that's correct.

NADLER: OK, so we'd have to make very clear that.

Mr. Steinhardt, you have suggested that -- in your written testimony you say that ECPA the -- whatever that was -- I forget the acronym -- should be amended to require the trap-and-trace/pen- register orders shall only be issued on the basis of an independent finding by judicial officers if there is reasonable cause to believe that the target of the order has or is about to commit a crime. By reasonable cause, you mean the same thing as probable cause, or you mean something different?

STEINHARDT: Well, it a slightly lesser standard that probable cause.

NADLER: OK, now you are suggesting that trap-and-trace and pen- registers for the Internet should have this higher standard than this simply certification that it's relevant to an investigation.

STEINHARDT: Yes, we're suggesting two things. One now is simply a certification; the judge has no discretion to turn down the request. And secondly, that there ought to be a high standard. Probably cause is fine with us, but there ought to be a high standard before the court issues that order, because, as you pointed out, this is an area where people do have a reasonable expectation of privacy and ought to have a reasonable expectation.

NADLER: And you're suggesting that for the Internet. You're not suggesting that for telephones?

STEINHARDT: We believe -- no, we are suggesting that for the telephone context as well.

NADLER: Because you believe that even in the telephone conversation -- telephone context, rather, the expectation of privacy is more substantial than the Supreme Court seemed to think it was 25 years ago?

STEINHARDT: Yes, I think clearly it is, yes.

NADLER: Why do you say clearly it is?

STEINHARDT: Well, I think most people would be very surprised to learn that they don't have a reasonable expectation of privacy in the numbers they dial, and the persons who call them. I think that's common sense. I think the Supreme Court decision defies common sense.

NADLER: Mr. Baker wants to say something on this.

BAKER: Yes. If I could add to that, in the -- when the Supreme Court wrote 25 years ago, it might have been true that you couldn't tell whether the call was completed, what was said and the like. But in the course of CALEA, the FBI has forced on the industry an enormous amount of transactional data gathering about calls other than content, which now can be obtained through trap-and-trace orders: how long you talked, whether you were on call waiting or call conferencing.

NADLER: Whether it was completed at all.

BAKER: Who conferenced in and when they got off. All that information would be part of a trap-and-trace order today.

NADLER: On telephones today, which was not the case and may in fact -- so the Supreme Court, if it were the same judges, using the same reasoning, might come to a different decision today because the facts are different.

STEINHARDT: I think many of us would think that they would, even in a telephone context, certainly in the Internet context. And Congress independently can certainly raise the standards for these things. Congress set the standard for this independently of the court.

NADLER: Well, let me just say, since my time is expiring, I appreciate this panel in panel in particular and I think that the Congress has to act because the history shows that police agencies cannot be afforded untrammeled discretion, and we cannot always assume their goodwill or even their lack of mistakes in protecting people's privacy.

CANADY: The gentleman's time has expired.

The gentleman from Georgia is recognized for five minutes.

BARR: Thank you, Mr. Chairman.

Mr. Sachs, is it correct to say that an Internet service provider -- if project Carnivore is forced on them, they have no control whatsoever over that program -- that device?

SACHS: That's my understanding, correct.

BARR: And no supervisory capability whatsoever?

SACHS: That's my understanding, correct.

BARR: Mr. Corn-Revere, did it surprise you, as I think it did -- I know it did me and I think it did Mr. Sachs also -- to have the government say that -- I think they said this, although they, of course, always waffle just a little bit -- that, in virtually every instance, the only reason for those 25 instances over the last two years in which they used project Carnivore was simply because the ISP provider refused to or could not satisfy them that they could provide the information they wanted in the way they wanted it?

CORN-REVERE: I have no idea what the government's experience was in those other 24 instances, but in the one example in which I was involved that certainly was not the case. The ISP did attempt to comply with the court order without the installation of **Carnivore** and ultimately was given no choice.

BARR: That's my impression, too.

If we could put back up on the board, Mr. Davidson, any one of your examples, and I'll come back to you in just a second.

But, Mr. Steinhardt, you're very familiar, and maybe some other members of the panel are also, with regard to a recent proposal by the government and by some of their colleagues up here in the House and the Senate to amend Fourth Amendment law, through amendments to a methamphetamine bill and the bankruptcy bill, to essentially carve out from the necessity for providing an inventory of seized items intangible information. Now, so far, knock on wood, we've been successful in stopping that from moving forward.

Is this the sort of data that the government would consider intangible so that they would, if they came in and seized it somehow, would not be required to tell you they've taken it?

STEINHARDT: Well, the capacity of the government to make creative arguments about what the law provides them in the way of investigatory tools never ceases to amaze me. So, yes, I think this is exactly the kind of information which they will make a claim is tangible and would be subject to those kinds of disclosures.

BARR: I would suspect so.

Mr. Davidson, with regard to your examples here, if you could just very briefly -- and this may be very elementary but I'm not familiar with all the details here -- which one is this? Example three. He went down to line 12 there that's in -- that's highlighted in, I guess, purple.

Are you saying that, in order for the government to get in and get that information, if that information is the target of what they're authorized to receive or on any e-mail they have to get in there to see if it is or it is not, that that means that they would also have to necessarily in every instance look at items one through 11?

DAVIDSON: Well, again, I think it's difficult to know exactly how their system works. It could be quite sophisticated. And there's a lot of -- well, the answer is, I think again, it depends.

DAVIDSON: They may be able to extrapolate from certain pieces of lines one through 11 what lines they need to look at in order to find this information. Again, this one is in the context of a communication with a web site.

But, yes, I think my general point was that they need to look at a fair amount of this packet in order to do the analysis to figure out what it is that they're entitled to.

BARR: Otherwise, there's no purpose to having Carnivore?

DAVIDSON: Exactly.

BARR: I mean, if Carnivore just sat there, fat, dumb and happy, and just waited for stuff to fall into its lap, it would never get anything. I mean, it has to go in there and look at this stuff somehow, doesn't it?

DAVIDSON: Right. And I think that there is a big question about whether or not that is a search in and of itself. There's a separate, sort of, kind of technical question, which is just to show how difficult this is and why we need to have some kind of real oversight, because there is all this investigation going on.

BARR: But would everybody agree that at this time, at least at this point, we need to probe further? We know so little about this and the ramifications and potential for abuse are so great, that -- and I forget who it was, that, sort of, times a wasting and we need to get in here and look at this to see exactly what it is, so that we can determine to what extent we need to refashion these, you know, very outdated laws.

DAVIDSON: I think that we would ask that Carnivore, you know, not be deployed without further, you know, public oversight and information about what's going on there. At the very least, some sort of independent review panel as a start.

BARR: To at least maintain the status quo without -- the pre- Carnivore status quo.

DAVIDSON: It's problematic enough.

BARR: Thank you.

CANADY: The gentleman's time is expired.

I want to thank all the members of this panel, again. And all the members of the subcommittee for your participation today. The testimony of the witnesses has been very helpful to us.

The subcommittee will stand in brief recess. This hearing has concluded.

END

NOTES:
Unknown - Indicates speaker unknown.
Inaudible - Could not make out what was being said.
off mike - Indicates could not make out what was being said.

LANGUAGE: ENGLISH

PERSON: CHARLES T CANADY (94%); HENRY J HYDE (72%); SPENCER THOMAS BACHUS (57%); LINDSEY GRAHAM (55%); BARNEY FRANK (54%); JOHN CONYERS JR (54%); MAXINE WATERS (54%); DAVID GREEN (53%); JERROLD NADLER (53%);

LOAD-DATE: July 27, 2000

FOCUS™
Search: General News;FBI and Carnivore

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

About LEXIS-NEXIS | Terms and Conditions | What's New
Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

WALL STREET JOURNAL

FBI Is Pressured To Disclose Codes For Carnivore

DATE 7-24-00
PAGE A6

By Ted Bridis
Staff Reporter of The Wall Street Journal

WASHINGTON-The Federal Bureau of Investigation is under increasing pressure to disclose the secret blueprints for its Carnivore surveillance system so independent technical experts can verify that the software monitors only the Internet communications of criminal suspects.

Despite mounting calls to permit such reviews, FBI officials maintain that disclosing the software's source code would allow hackers to find ways to defeat the system. The officials also argue that such a disclosure could violate copyright protections because Carnivore includes portions of software code from a product licensed to the government by an unidentified vendor.

Congress is expected to press senior FBI officials on the subject at a hearing today before a House Judiciary Committee panel led by Florida Republican Rep. Charles T. Canady. Lawmakers have indicated that they would seek assurances from the bureau that e-mails from innocent citizens aren't gobbled up whenever a federal judge agrees that the FBI can plug Carnivore into an Internet service provider's network.

One scheduled witness for the hearing, Matthew Blaze, an AT&T Corp. researcher, says the FBI's failure to fully disclose how Carnivore works has contributed to an "atmosphere of mistrust and confusion."

In an essay published on the Internet last week, Mr. Blaze wrote that releasing the system's source code "is a critical first step in assuring the public that Carnivore can at least be configured to do what it is supposed to do." Mr. Blaze questioned Carnivore's effectiveness, suggesting that even modest electronic forgery or data-scrambling techniques could foil it, and described conditions under which it could mistakenly capture e-mails and other communications intended for innocent users.

While the FBI is resisting calls for broad disclosure of the source code-already the target of at least two requests under the Freedom of Information Act-the bureau has sought to assuage fears by describing in remarkable detail how the system works. On Friday, dozens of reporters crowded a conference room at FBI headquarters to watch a demonstration.

The bureau has also proposed a compromise, tentatively agreeing to an examination of Carnivore by university researchers who would promise not to disclose its blueprints.

The American Civil Liberties Union, one of the groups that has requested the source code, said it might agree to such an offer if the FBI gives the blueprints to the ACLU and lets it select the experts.

Doc. #15

USA TODAY

DATE 1-24-00

PAGE 11A

Today's debate: FBI and Internet privacy

FBI eavesdrops on e-mail, crashes privacy barriers

Our view:

Agency says it targets criminals. History says it can't be trusted.

The FBI has a knack for concocting colorful code names for crime-busting toys. The latest is "Carnivore" — an eavesdropping device that devours private e-mail and spits out interesting parts for scrutiny. Not just criminals' e-mail. Anyone's e-mail.

The FBI already has attached Carnivore to the e-mail hardware at some Internet service providers. Though it won't say where, the FBI says the tool has been used fewer than 25 times. Once it's in place, Carnivore acts as an unrestrained Internet wiretap, snooping through every Internet communication that comes within its reach.

The House Judiciary Committee will hold a hearing today, at which it will ask the FBI to explain its actions. But in the 15 weeks since Carnivore was revealed in obscure congressional testimony, the bureau has evaded answers about both its capabilities and proposed uses. The bureau won't answer even the most basic questions about whom the technology targets and how it protects the privacy of innocent Internet users. The potential for abuse is unprecedented:

▸ **Who.** Carnivore is intended to rifle through potential criminals' Internet traffic after police obtain a court order. But the tool gives the FBI the ability to track not just the individual named in the court order, but also everyone who uses the same server at the Internet service provider. At America Online, for example, that would be thousands of people. What's to keep the FBI from snooping more broadly? Only its own assurances.

▸ **What.** Coverage so far has focused on the surveillance of e-mail, but a program that can snoop through e-mail can just as easily eavesdrop on Web surfing, since the information travels in similar forms over the same servers. What information will the FBI collect about the sites people visit and even the ads they click on?

▸ **When.** The FBI admits that Carnivore is more invasive than a conventional phone tap. Yet it faces no more restraints than those that protect telephone conversations, which are themselves inadequate. Since Carnivore is a greater threat to privacy, shouldn't there be more restrictions on when it's used?

▸ **Why.** The Congressional testimony that revealed the existence of Carnivore also disclosed two other systems used by the FBI for similar purposes: "Omnivore" and "Etherpeek." Why weren't those revealed earlier? How many times have they been used and for what purpose?

The FBI's response to those questions is, in essence, trust us; we're only after criminals and terrorists. But even a cursory glance at law-enforcement history shows that promise can't be trusted. The temptation of government to collect and misuse information is irresistible. (See box.)

Further, the FBI shows no inclination to exercise restraint. In every aspect of electronic privacy — computers, the Internet and cellphones — it has pushed invasiveness to the technological limit:

▸ In 1994, the FBI lobbied to have backdoor access installed in every new computer to ease electronic snooping, allowing the FBI to defeat security. The plan was dropped after the National Academy of Sciences determined such access would make all computers more vulnerable to illegal break-ins.

▸ In 1995, the bureau asked for the capability to tap as many as one in 100 phones in major cities. It backed off only after a public outcry. Lacking such technology, no totalitarian state in the world is that invasive.

▸ In 1996, the FBI proposed liberalizing the export of encryption programs, but only for companies that, under court order, make available "keys" to defeat the privacy programs. After two federal courts struck down the proposal, the administration gave up.

▸ In 1997, the FBI went to court to protect a plan that would allow cellphones to be used by police to locate the positions of their users. The case remains in court today.

▸ Today, the thin answers the FBI has made public about Carnivore raise more disturbing questions. An explanation of Carnivore posted on the FBI's Web site casually discusses the electronic surveillance of an entire "facility," without explaining how broad such e-snooping could be.

In each case, the FBI gets convenience. The public gets government intrusion on a scale unequaled in constitutional history. Abuse will only expand as less-closely watched law enforcement agencies piggyback on the technology.



By Quin Tian, USA TODAY

FBI fumbles privacy

The FBI has a long history of violating the privacy of U.S. citizens, often with political motives. Some examples:

▸ 1956: The FBI rifled credit files and criminal records of 43 ordinary Delaware citizens called to jury duty in a politically sensitive case. Many also were investigated for ties to the NAACP.

▸ 1960s: FBI wiretapped Martin Luther King Jr. to gather damaging information on extramarital affairs.

▸ 1970: FBI sent damaging information on NAACP chief, Rev. Ralph Abernathy, to Vice President Spiro Agnew.

▸ 1980s and '90s: FBI kept a file on AIDs activist group ACT UP and its planned protests.

▸ 1993 and '94: The FBI "inadvertently" released files containing unsubstantiated allegations on numerous Republicans to low-level political appointees of the Clinton administration.

Attorney General Janet Reno said last week that she intends to begin a thorough review of Carnivore. That's a positive step, but it's hard to understand how Reno wouldn't already have a complete knowledge of the tool since she is the head of the "President's Working Group on Unlawful Conduct on the Internet," which just completed its report in March.

The Clinton administration greeted howls about Carnivore's reach with a proposal to update electronic-privacy laws, although congressional Democrats say the bill has no chance of even being voted on this year.

The time for such updating and review was before Carnivore was used. Carnivore needs to be shut down until an outside review of its capabilities and safeguards is complete. And the Internet companies that willingly complied with the FBI's use of the technology in the past need to come forward and inform individuals whose e-mail the FBI "filtered."

Of course, law enforcement agencies cannot operate without ways to monitor the modern communications tools of criminals. But even a cursory glance at the FBI's history shows it can't be trusted to make privacy for everyone else a priority.

Doc #16

The right of the innocent to be free from government intrusion should not be compromised to make life easier for the FBI. Until the bureau can show that its new technology poses no threat to the public, Carnivore needs a starvation diet.

Technology used narrowly

Opposing view:
Court order required to intercept only specific e-mails of criminals.

By John E. Collingwood

First, let's get the facts straight. The FBI and all other law enforcement agencies can intercept e-mails only pursuant to a court order signed by a judge who is satisfied that the government has demonstrated probable cause that a serious crime is being or has been committed, that the e-mails will be about that crime, and that the interception is necessary to obtain evidence about the crime.

Conducting an intercept beyond that is a federal crime subject to severe criminal and civil sanctions. The entire process requires continuous reporting to a court and, of course, ultimately is subject to vigorous challenge by defense attorneys. Even when only address information is sought, a court order is still required.

What does "Carnivore" do? In the simplest terms, it ensures that only the exact communications authorized by the court to be intercepted are intercepted. So, for example, if a court authorizes only the interception of e-mail from a particular drug dealer to another drug dealer, this system captures only that e-mail to the exclusion of all other communications, regardless of whom sends them and where they are going. Nothing else is monitored or collected, and everything collected is supervised by the court.

When is Carnivore used? It is used only when an Internet service provider cannot, on its own, effect the interceptions consistent with a narrow court order. Accordingly, it has been used very few times, predominately in terrorism cases.

In 1968, Congress spelled out strict requirements for interceptions. Carnivore simply ensures that law enforcement agencies comply precisely with those requirements as technology advances. We understand why certain segments oppose this court-supervised technique. But since 1968, because of this law, many lives have been saved and thousands of drug dealers, terrorists, child predators and spies are in jail.

The chairman of PSINet laid out the appropriate challenge. He does not want to see Carnivore on his network unless we can prove it collects only the traffic from the target of a court order. That, of course, is precisely what Carnivore does, electronically protect the privacy of those not subject to the court order.

John E. Collingwood is an assistant director of the Federal Bureau of Investigation.

Doc #17

July 24, 2000

Mr. Brian Gallagher
Editor of the Editorial Page
USA Today
1000 Wilson Blvd.
Arlington, VA 22229

Dear Mr. Gallagher:

In response to today's editorial about "Carnivore," again let's get the facts correct.

USA Today rightly points out that "law enforcement agencies cannot operate without ways to monitor the modern communications tools of criminals" but then questions who should ensure that privacy is properly protected. The simple answer is the same as it has been for over 30 years--federal judges. All of the federal criminal and civil sanctions and judicial oversight that apply to wiretapping and have effectively protected those not the target of a court order apply to the use of Carnivore to intercept the e-mails of criminals.

Unlike as the editorial reflects, however, Carnivore does not snoop through every Internet communication, does not spit out everyone's e-mail, and is not an unrestrained Internet wiretap. Court orders authorizing the intercept of criminals' e-mails come only after rigorous review and the conclusion that there is probable cause that a crime is being or has been committed, the e-mails are about or in furtherance of that crime and the intercept is necessary to gather evidence about the crime. The orders are specific as to whom and what can be intercepted and then the courts supervise the interception to ensure compliance. Evading those court orders is a serious crime which would, of course, produce absolutely nothing of evidentiary value.

Finally, the editorial says the "Bureau won't answer even the most basic questions about whom the technology targets and how it protects the privacy of innocent users." Contrary to

1 - Mr. Pickard
1 - Dr. Kerr
1 - Mr. Parkinson
1 - Mr. Collingwood
JEC:mmc (8)

1 - [redacted]
1 - [redacted]

66-1
67C-1

Doc. #18

that assertion, however, the FBI has shown the system to and answered these questions for dozens of people on Capitol Hill and over 30 reporters representing 25 media outlets. USA Today, of course, was invited and today we are anxious to present it at an open hearing before a congressional subcommittee. We are arranging for an independent review as well.

Sure Carnivore can be controversial and clearly is ill-named. But it is used only pursuant to court order; has been used sparingly, predominantly in terrorism cases, and then only when an Internet Service Provider cannot on its own comply with the court order; and, when used, collects only what the law authorizes and the courts instruct be collected--evidence about serious crime that cannot be otherwise gathered.

Sincerely yours,

John E. Collingwood
Assistant Director
Office of Public and
Congressional Affairs

5/24/02 Release - Page 125

USA TODAY

DATE: 7-25-00

PAGE: 3-D

Uproar worse than bite of this FBI beast



By Quin Tran, USA TODAY

eLife

By Elizabeth Weise

Carnivore might sound like a particularly violent computer game, or perhaps a movie that you wouldn't let your 12-year-old go see alone. It's actually a project of the FBI, which, depending on your outlook, is either a threat to the privacy of all Americans or a useful tool in fighting criminals.

The unfortunately named program (the FBI has been trying to come up with something else since news of its existence broke) is an eavesdropping device housed in a tangle of electronics the size of a laptop.

The agency wants to deploy Carnivore boxes at the main computers of all Internet service providers, to provide an efficient way for the FBI to conduct court-approved wiretaps on e-mail in an era when all communication, lawful and otherwise, is going digital.

Since word of this hit during congressional testimony, the nation's privacy advocates have been outraged at the idea of the Internet being "bugged."

But it's not just activists who are up in arms. So is the Republican leadership in Congress. House Majority Leader Dick Armey of Texas has attacked Carnivore as being illegal under current wiretap laws, and the Constitution subcommittee of the House Judiciary Committee held hearings Monday to look into the matter.

Now, privacy advocates have been fighting for years to protect our information from prying eyes. But it's fascinating to see everyone else getting into such a lather over a system that — unless the FBI is lying through its teeth — is very limited in what it's allowed to do.

In a perfect world, I might be concerned about the idea that were I the subject of an investigation, the FBI could monitor my e-mail. But agents would at least have to go before a judge and get permission. And even at the height of government surveillance during the McCarthy era, the number of people being monitored numbered well under 1 million.

That pales in comparison with what's already happening with every keystroke we make as we wander the commercial Web.

Many sites record every search made and every mouse click, building up a detailed dossier of interests and surfing choices, which they use to target the ads that appear on our screens.

A fair number also "bug" their sites, scattering invisible cookies that our browsers pick up, allowing that site and others to share information to create an even more specific portrait.

In addition, by linking to outside databases, it's possible to attach that portrait to a name, address and personal data, including what stores you shop at, what you buy and when you pay your bills. And let's not forget that if the company goes out of business, it can try to auction off its database to the highest bidder — though the government we so fear is working on making that illegal.

All that is bad enough, but it's nothing compared with what will happen when the Web goes wireless and we all begin accessing our e-mail, bank accounts and stock funds from cellphones. If you thought a cookie or two was intrusive, wait till everything you do is linked in real time to your phone number and exact physical location, as cellphones soon will be.

This isn't to say Carnivore shouldn't be carefully monitored or that we should trust the FBI just because it tells us to. I just don't understand why so many of the people up in arms over Carnivore rail against passing any kind of legal protection for consumer privacy online, saying the industry will develop only if it's left to self-regulate.

When it comes to the privacy of my personal information, I trust the government, which is bound by strict laws, a whole lot more than I trust multinational corporations.

22

Doc. #19

USA TODAY

DATE: 7-25-00
PAGE: 10-A

FBI defends e-mail surveillance tool

By Kevin Johnson
USA TODAY

WASHINGTON — Peppered with questions from skeptical lawmakers, the FBI played down concerns Monday that its e-mail surveillance program known as "Carnivore" could be used to eavesdrop on the innocent.

At a House Judiciary subcommittee hearing that seemed to capture both the promise and pitfalls of new technology for law enforcement, Assistant FBI Director Donald Kerr defended the program as a useful tool for agents. He said any surveillance done with the Carnivore program is limited to those suspects named in court orders.

Critics, including an unusual coalition of conservative Republicans and civil liberties advocates, have complained that the program could be used to do broad surveillance.

Their fear stems from the way the FBI implements the Internet-wiretapping system. Carnivore works through a suspect's Internet service provider, such as America Online. It allows investigators to identify and view a suspect's e-mails among all e-mails moving through the provider's system.

Critics are concerned about giving law enforcement access to the e-mails of innocent people as well as suspects. Although Carnivore can retrieve any e-mails, investigators are restricted to those that have been approved for monitoring by a judge.

House Judiciary Committee Chairman Henry Hyde, R-Ill., said the Carnivore debate reflected an ongoing tension between law enforcement and individual rights.

"You can understand people's concerns for privacy? There are people who are skeptical about this culture of privacy and how porous it is," Hyde told Kerr and other FBI officials at the House hearing.

Meanwhile, Rep. J.C. Watts, R-Okla., urged the Clinton administration to suspend the program, under which the FBI has intercepted e-mails in 25 probes over the past two years. No cases involving Carnivore have come to trial.

Justice Department officials also said they are reviewing the program to make sure that federal agents have not been involved in unlawful eavesdropping. Kerr said investigators involved in the Carnivore program have never been provided Internet traffic outside the scope of their probes: "We don't do broad searches (on Internet traffic) and surveillance that is not authorized by court order."

This year, the program has been used in 16 cases: six criminal probes and 10 national-security investigations.

21

Doc # 20

July 25, 2000

Ms. Christine Bertelson
Editor of Editorial/Opinion Page
St. Louis Post Dispatch
900 North Tucker Blvd
St. Louis, MO 63101-1099

Dear Ms. Bertelson:

In response to your recent editorial "Silent cybercrime hunting," a few additional facts might help your readers understand the safeguards and judicial oversight applicable to the interception of e-mail on the Internet.

As always happens, dangerous criminals and terrorists use new technology as fast as anyone does. So now, instead of telephones, we increasingly find criminals communicating by e-mail in furtherance of their crimes. We have seen this in everything from child pornography to terrorism. That is why the FBI developed the Carnivore program, a tool that permits surgical interceptions in the midst of the flood of data on the Internet.

To use Carnivore to obtain a criminal's e-mail, the FBI first must successfully demonstrate to a judge that there is probable cause to believe that a serious crime is being or has been committed, the e-mails are about or in furtherance of that crime, and the interception is necessary to gather evidence about the crime. It is the same rigorous legal standard that applies to the interception of telephone conversations. The same severe criminal and civil sanctions apply to any misuse as well, and the whole process is supervised beginning to end by the federal court issuing the order. Finally, the use of this evidence and the method of collection are always subject to vigorous challenge by defense lawyers.

The FBI only uses Carnivore when an Internet Service Provider cannot, on its own, provide the very limited information authorized by courts to be intercepted, e.g., e-mails to and from two drug dealers. That is why it has only been used 25 times since it was developed and, in these cases, it was used with assistance from the Internet Service Provider.

1 - Mr. Pickard
1 - Dr. Kerr
1 - Mr. Parkinson
1 - Mr. Collingwood
JEC:mmc (9)

1 [redacted]
1 [redacted]
1 [redacted]

66-1
67C-1

DOC. #21

Ms. Christine Bertelson

Finally, Carnivore does not "automatically" search for "key words among all e-mail traffic." It does not search the content of e-mail at all. To search as the editorial suggests would be contrary to federal law, subject to severe criminal sanctions and produce nothing of evidentiary value because it would contravene the parameters of the Fourth Amendment. Instead, Carnivore ensures that law enforcement only gets those specific e-mails addressed as described in the court's order to the complete exclusion of everything else on the Internet.

Sincerely yours,

John E. Collingwood
Assistant Director
Office of Public and
Congressional Affairs

(Mount Clipping in Space Below)

(Indicate page, name of newspaper, city and state.)
Editorial Page, St. Louis Post Dispatch, St. Louis, Mo.

Date: 7/24/2000
Edition: Final *****

Title:

Character:
or
Classification:
Submitting Office: St. Louis

Indexing:

PRIVACY

Silent cybercrime hunting

WITH a staggering 1.4 billion e-mails exchanged each day, Internet technology has raced around and ahead of laws governing traditional forms of communication and commerce. That is part of the Internet's appeal, but also part of its danger. Many of the 2.2 million Americans who talk and shop on-line were less than happy to hear that the Federal Bureau of Investigation has been using an e-mail patrol system with surveillance capabilities far beyond those of telephone wiretaps.

Most citizens feel reasonably comfortable with Fourth Amendment protections and laws that allow phone call traces and wiretaps of suspected criminals. But Internet communications are vulnerable in a different way. The FBI's "Carnivore" system, named for its ability to hunt down "meat," automatically searches for key words among all the e-mail traffic of a suspect's Internet service provider. That creates an enormous potential for abuse and loss of privacy.

The White House and Congress, ever late in chasing cyber-issues, are considering legislative proposals to create Internet privacy protections comparable to those governing telephone conversations and the search and seizure of personal papers. But Internet communication — some along telephone lines, some along cable television wires — makes it a staggering task. A House judiciary subcommittee plans to hold hearings today to weigh law enforcement needs and constitutional privacy rights, and to examine the extent to which current laws let the government use devices like Carnivore.

The FBI says it has used Carnivore less than 50 times in the year it has been available, mostly to stalk suspected cases of hacking, intrusion and some counter-terrorism. Clearly, criminals can't be allowed to use the Internet as a safe haven for communications that authorities have been able to monitor for years on the telephone. But silent government sifting of the nation's e-mail is not acceptable. We urgently need new laws that protect citizens both from criminal suspects and invasions of privacy.

Doc # 22 TOTAL P.02

Department of Justice

STATEMENT

OF

KEVIN V. DI GREGORY

DEPUTY ASSISTANT ATTORNEY GENERAL

CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON THE CONSTITUTION

COMMITTEE ON THE JUDICIARY

UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

"CARNIVORE" AND THE FOURTH AMENDMENT

PRESENTED ON

JULY 24, 2000

Doc. #23

STATEMENT OF
KEVIN V. Di GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE
BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION
OF THE HOUSE COMMITTEE ON THE JUDICIARY
on
"CARNIVORE" AND THE FOURTH AMENDMENT

July 24, 2000

Mr. Chairman and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment. On April 6, 2000, I had the privilege of testifying before you during a hearing on Internet privacy and the Fourth Amendment; I am pleased to continue to participate in the discussion today about "Carnivore" and its role in protecting individual privacy on the Internet from unwarranted governmental intrusion, and about the critical role the Department plays to ensure that the Internet is a safe and secure place.

Privacy and Public Safety

It is beyond dispute that the Fourth Amendment protects the rights of Americans while they work and play on the Internet just as it does in the physical world. The goal is a long-honored and noble one: to preserve our privacy while protecting the safety of our citizens. Our founding fathers recognized that in order for our democratic society to remain safe and our liberty intact, law enforcement must have the ability to investigate, apprehend and prosecute people for criminal conduct. At the same time, however, our founding fathers held in disdain the government's disregard and abuse of privacy in England. The founders of this nation adopted the Fourth Amendment to address the tension that can at times arise between privacy and public

safety. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. The Electronic Communications Privacy Act ("ECPA") establishes a three-tier system by which the government can obtain stored information from electronic communication service providers. In general, the government needs a search warrant to obtain the content of unretrieved communications (like e-mail), a court order to obtain transactional records, and a subpoena to obtain information identifying the subscriber. *See* 18 U.S.C. §§ 2701-11.

In addition, in order to obtain source and destination information in real time, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. *See* 18 U.S.C. 3121, et seq.

Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510-22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.

The safeguards for privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement, clarifying what is acceptable evidence

gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in preserving privacy. When law enforcement investigates, successfully apprehends and prosecutes a criminal who has stolen a citizen's personal information from a computer system, for example, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emerging technologies that are changing the face of communications. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

Law Enforcement Tools in Cyberspace:

Although the Fourth Amendment is over two centuries old, the Internet as we know it is still in its infancy. The huge advances in the past ten years have changed forever the landscape of society, not just in America, but worldwide. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. As has been the case with every major technological advance in our history,

however, we are seeing individuals and groups use this technology to commit criminal acts. As Deputy Attorney General Eric Holder told the Crime Subcommittee of this Committee in February, our vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

To satisfy our obligations to the public to enforce the laws and preserve the safety, we use the same sorts of investigative techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional, statutory, internal and court-ordered boundaries. Carnivore is simply an investigative tool that is used online only under narrowly defined circumstances, and only when authorized by law, to meet our responsibilities to the public.

5/24/02 Release - Page 135

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling. To investigate this, it is helpful to determine who is communicating with the drug dealer. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager, and either the telephone company or law enforcement would have installed these devices to comply with the court's order. Thereafter, the source and destination of his phone calls would have been recorded. This is information that courts have held is not protected by any reasonable expectation of privacy. Given the personal nature of this information, however, the law requires government to obtain an order under these circumstances. In this way, privacy is protected and law enforcement is able to investigate to protect the public.

Now, that same drug dealer may be just as likely to send an e-mail as call his confederates. When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like Carnivore.

When a criminal uses e-mail to send a kidnaping demand, to buy and sell illegal drugs or to distribute child pornography, law enforcement needs to know to whom he is sending messages and from whom he receives them. To get this information, we obtain a court order, which we

serve on the appropriate service provider. Because of the nature of Internet communications, the addressing information (which does not include the content of the message) is often mixed in with a lot of other non-content data that we have no desire to gather. If the service provider can comply with the order and provide us with only the addressing information required by court order, it will do so and we will not employ Carnivore. If, however, the service provider is unwilling or unable to comply with the order, we simply cannot give a criminal a free pass. It is for that narrow set of circumstances that the FBI designed "Carnivore."

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather only the email addresses of those persons with whom the drug dealer is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. In other words, Carnivore is a *minimization* tool that permits law enforcement strictly to comply with court orders, strongly to protect privacy, and effectively to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

As with any other investigative tools, there are many mechanisms we have in place to prevent against possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment, of course, restricts what law enforcement can do with Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act, and the courts.

For federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example,

before Carnivore may be used to intercept wire or electronic communications, the requesting investigative agency must obtain approval for the Title III application from the Department of Justice. Specifically, the Office of Enforcement Operations (OEO) in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. Even if the proposal clears the OEO, approval must be given by a Deputy Assistant Attorney General. Although this requirement of high-level review is required by Title III only with regard to proposed intercepts of wire and oral communications, the Department voluntarily imposes the same level of review for proposed interceptions of electronic communications (except digital-display pagers). Typically, investigative agencies such as the Federal Bureau of Investigation have similar internal requirements, separate and apart from Constitutional, statutory or Department of Justice requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be approved by the proper court. The court will evaluate the application under the Fourth Amendment and using the familiar standards of Title III. By statute, for example, the application to the court must show, through sworn affidavit, why the intercept is necessary as opposed to other less-intrusive investigative techniques. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court.

Courts also often impose their own requirements. For example, many federal courts require that the investigators provide periodic reports setting forth information such as the number of communications intercepted, steps taken to minimize irrelevant traffic, and whether the interceptions have been fruitful. The court may, of course terminate the interception at any time.

The remedies for violating Title III or ECPA by improperly intercepting electronic communications can include criminal sanctions, civil suit, and for law enforcement agents, adverse employment action. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Carnivore itself also contains self-regulating features. For example, because of its sophisticated passive filtering features, it automates the process of minimization without intrusive monitoring by investigators, and simply disregards packets of information that do not satisfy the criteria in the court's authorization. Indeed, one of the most powerful privacy-protecting features of Carnivore is its ability to ignore information that is outside the scope of the court-ordered authority. For later verification, it also logs the filter settings. In addition, as a practical matter, Carnivore is not deployed except with close cooperation with the appropriate system provider. In any event, the FBI does not use Carnivore in every instance in which the court orders a Title III electronic communication intercept. Indeed, I understand that the Bureau uses Carnivore only in those instances when the service provider is unable to comply with the court order using its own equipment, or when the provider asks the FBI to use Bureau equipment.

As I testified in April, we face three major categories of challenges in trying to keep the Internet a safe and secure place for our citizens. These are:

1. Technical challenges that hamper law enforcement's ability to locate and prosecute criminals that operate online;
2. Certain substantive and procedural laws that have not kept pace with the changing technology, creating significant legal challenges to effective investigation and prosecution of crime in cyberspace; and
3. Resource needs that must be addressed to ensure that law enforcement can keep pace with changing technology and has the ability to hire and train people to fight cybercrime.

Carnivore is an investigative tool that assists us in meeting the first challenge. As we have witnessed, tracking a criminal online is not always an impossible task using our investigative tools. For example, last year federal and state law enforcement combined to successfully apprehend the creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California. Although we are proud of these important successes, we still face significant challenges as online criminals become more and more sophisticated.

In nearly every online case, tracking the online criminal requires law enforcement to attempt to trace the "electronic trail" from the victim back to the perpetrator. In effect, this "electronic trail" is the fingerprint of the twenty-first century -- only much harder to find and not as permanent as its more traditional predecessor. In the physical world, a criminal and his victim are generally in the same location. But cybercriminals do not have to physically visit the crime scene. Instead they cloak their illegal activity by weaving communications through a series of

anonymous remailers, by creating forged e-mail headers with powerful point and click tools readily downloadable from hacker websites, by using a "free-trial" account or two, or by "wiping clean" the logging records that would be evidence of their activity.

In some cases, the criminal may not even be in the same country as the victim. The global nature of the Internet, while one of the greatest assets of the Internet to law-abiding citizens, allows criminals to conduct their illegal activity from across the globe. In these cases, the need to respond quickly and track the criminal is increasingly complicated and often frustrated by the fact that the activity takes place throughout different countries. With more than 190 countries connected to the Internet, it is easy to understand the coordination challenges that face law enforcement. Furthermore, in these cases, time is of the essence and the victim may not even realize they have been victimized until the criminal has long since signed-off. Clearly, the technical challenges for law enforcement are real and profound.

This fact was made clear in the findings and conclusions reached in the recently released report of the President's Working Group on Unlawful Conduct on the Internet, entitled, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." This extensive report highlights in detail the significant challenges facing law enforcement in cyberspace. As the report states, the needs and challenges confronting law enforcement, "are neither trivial nor theoretical." The Report outlines a three-pronged approach for responding to unlawful activity on the Internet:

1. Conduct on the Internet should be treated in the same manner as similar conduct offline, in a technology neutral manner.

2. We must recognize that the needs and challenges of law enforcement posed by the Internet are substantial, including our need for resources, up-to date investigative tools and enhanced multi-jurisdictional cooperation.

3. Finally, we need to foster continued support for private sector leadership in developing tools and methods to help Internet users to prevent and minimize the risks of unlawful conduct online.

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report can be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at www.cybercrime.gov. In addition to the report, www.cybercrime.gov also contains other useful information on a wide array of Internet related issues, including the topic of today's hearing – privacy.

Despite the type of difficulties outlined in the Unlawful Conduct Report and discussed today, the Justice Department and law enforcement across this nation are committed to continuing to work together and with their counterparts in other countries to develop and implement investigative strategies to successfully track, apprehend, and prosecute individuals who conduct criminal activity on the Internet. In so doing, the same privacy standards that apply in the physical world remain effective online.

Mr. Chairman, the Department of Justice has taken a proactive leadership role in making cyberspace safer for all Americans. The cornerstone of our cybercrime prosecutor program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and became a Section in 1996. CCIPS

has grown from five attorneys in 1996 to nineteen today, and we need more to keep pace with the demand for their expertise. The attorneys in CCIPS work closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators," or CTC's, in U.S. Attorney's Offices around the nation. Each CTC receives special training and equipment and serves as the district's expert on computer crime cases. CCIPS and the CTC's work together in prosecuting cases, spearheading training for local, state and federal law enforcement, working with international counterparts to address difficult international challenges, and providing legal and technical instruction to assist in the protection of this nation's critical infrastructures. We are very proud of the work these people do and we will continue to work diligently to help stop criminals from victimizing people online.

I also note that public education is an important component of the Attorney General's strategy on combating computer crime. As she often notes, the same children who recognize that it is wrong to steal a neighbor's mail or shoplift do not seem to understand that it is equally wrong to steal a neighbor's e-mail or copy a proprietary software or music file without paying for it. To remedy this problem, the Department of Justice, together with the Information Technology Association of America (ITAA), has embarked upon a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. The "Cybercitizen Awareness Program" seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children an understanding of cyberspace benefits and responsibilities, an awareness of consequences resulting from the misuse of the

5/24/02 Release - Page 143

medium and an understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed.

Finally, Mr. Chairman, the Subcommittee may be aware that the Administration will soon be transmitting to Congress a legislative proposal addressing various issues relating to cyber-security. I know that the focus of today's hearing is the Carnivore program, and this is not the time to undertake any detailed discussion of the Administration's proposal. I would, however, like to mention two points that relate directly to today's discussion. First, the Administration supports raising the statutory standards for intercepting the content of electronic communications so they are the same as those for intercepting telephone calls: high-level approval, use only in cases involving certain predicate offenses that are specified by statute, and statutory suppression of evidence derived from improper intercepts. Second, the Administration supports requiring federal judges to confirm that the appropriate statutory predicates have been satisfied before issuing a pen register or trap-and-trace order. Those changes would apply to the use of Carnivore -- and would, in important respects, simply confirm by statute the policies and procedures already followed by the Department of Justice. Beyond those specific points, I will simply note here that the Administration supports a balanced updating of laws to enhance protection of both privacy and public safety, and that the forthcoming proposal will contain important provisions whose enactment would be most helpful in the ongoing fight against cyber-crime.

Conclusion:

Mr. Chairman, I want to thank you again for this opportunity to testify today about our efforts to fight crime on the Internet while preserving the rights conferred by the Fourth Amendment and statute. Ultimately, the decision as to the appropriate parameters of law

5/24/02 Release - Page 144

enforcement activity lies squarely within the Constitution and the elected representatives of the people, the Congress. The need to protect the privacy of the American people, not just from the government but also from criminals, is a paramount consideration, not just in the context of the Internet, but in general. The Department of Justice stands ready to work with this Subcommittee and others to achieve the proper balance between the important need for protecting privacy and the need to respond to the growing threat of crime in cyberspace.

Mr. Chairman, that concludes my prepared statement. I would be pleased to attempt to answer any questions that you may have at this time.

5/24/02 Release - Page 145

ORAL STATEMENT OF KEVIN DI GREGORY

Mr. Chairman, and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment.

We have seen magnificent growth of the Internet over the last ten years. It has created vast benefits for citizens, businesses and governments, and seems to hold boundless promise if we can harness it. The Internet has spurred a new and thriving economy. Many businesses have prospered by providing their products and services through the Internet. Others have assisted in building, maintaining and improving the Internet itself. The Internet has given people jobs, supported families and communities and created new opportunities for commerce for America and the world. The Internet has touched both our working lives and our family lives.

As we have seen throughout history, however, there are those who use the powerful tools of progress to inflict harm on others. The Internet has not escaped this historical truth. Even in the Internet's relatively short existence we have seen a wide range of criminal use of the technology. It has been used to commit traditional crimes against an ever widening number of victims. There are also those criminals intent on attacking and disrupting computers, computer networks and the Internet itself. In short, although the Internet provides an unparalleled opportunities for Americans to freely express ideas, it also provides a very effective means for ill-motivated persons to breach the privacy and security of others.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for

5/24/02 Release - Page 116

criminal activity. If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

Despite the fervor over the unfortunately-named "Carnivore," the truth of the matter is that Carnivore is in reality a tool that helps us achieve this balance. To satisfy our obligations to the public to enforce the laws and preserve public safety, we use the same sorts of investigatory techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional and legal limits. Carnivore is simply an investigatory tool that helps us to investigate online in the same way as in the physical world, and enables us to obtain **only** the information we are authorized to obtain through a court order.

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling his goods. It is therefore important to determine with whom the drug dealer is communicating. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager. Now, that same drug dealer, or a kidnapper or a child

pornographer, may be just as likely to send an e-mail as to call his confederates.

When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. It is for that narrow set of circumstances that the FBI designed "Carnivore." Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like Carnivore.

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather pursuant to an order only the email addresses of those persons with whom the drug dealer is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. In other words, Carnivore is a minimization tool that permits law enforcement to comply with court orders, to protect privacy, and to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

And as with any other investigative tools, there are many mechanisms we have in place to prevent possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment and the courts, of course, restricts what law enforcement can do on line, with or without Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act.

In the case of federal Title III applications, the Department of Justice imposes its own

guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example, before Carnivore may be used to intercept wire or electronic communications, with the limited exception of digital display pagers, the requesting investigatory agency must obtain approval for the Title III application from the Department of Justice. Specifically, the Office of Enforcement Operations in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. If the proposal clears the OEO, approval must generally be given by a Deputy Assistant Attorney General. Typically, investigative agencies such as the Federal Bureau of Investigation have similar but separate internal requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be approved by the proper court using familiar but exacting standards. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court. And courts also often impose their own additional requirements.

In addition, the remedies for violating Title III or ECPA by improperly intercepting electronic communications include criminal sanctions and civil suits. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Despite this panoply of protections, we recognize that concerns remain about this tool. Therefore, the Attorney General has asked for an independent review of the Carnivore source code to ensure that its capabilities are what we understand them to be. A report generated from the review will be publicly disseminated to interested groups within industry, academia and elsewhere, and should alleviate any concerns regarding unjustified intrusions on privacy from the

use of this tool.

Conclusion

Mr. Chairman, my testimony today necessarily highlights a few of the more significant aspects of the balance between privacy and security. The Department of Justice has provided the Committee with my full written statement. It is my sincere hope and expectation that through this and other fora, those of us who are concerned about privacy and public safety will recognize that responsible law enforcement can enhance both goals.

5/24/02 Release - Page 150

The New York Times

DATE: 7-27-02
PAGE: A26

Wiretapping in Cyberspace

Millions of Americans now log on to the Internet as naturally and as frequently as they pick up a phone. Technology has created a revolution in personal communications, but technology is also making it possible for government and even employers to monitor private conversations as never before. Telephone-era laws must be updated to address these new challenges to privacy.

Last week the White House proposed some limited changes to the federal wiretap and electronic privacy laws that would raise legal standards for government interception of e-mail. Separately, several lawmakers introduced legislation to require employers to notify employees about how e-mail, Internet use and phone calls are monitored. Employees of The New York Times Company are already notified that the company reserves the right to review e-mail messages while investigating a complaint. Last year the company dismissed 23 employees — most based at a regional business office — for sending offensive e-mail messages.

In the absence of more stringent controls, law enforcement agencies may be tempted to conduct wholesale monitoring of digital written communications. It is probably not practical for agents to listen in on all the phone calls, for example, that go through AT&T. But new technology is making it possible for agencies like the F.B.I. to scan, read and record millions of pieces of e-mail on the network of an Internet service provider. Until now, this kind of power and its potential for abuse were not so readily available.

Current wiretapping laws were not drafted with this technology in mind and need to be updated. Various statutes now set different legal standards for the secret interception of domestic communications by law enforcement agencies, depending on whether the communication is by telephone, e-mail or cable modem.

The Clinton administration is proposing to eliminate these inconsistencies. Its plan would bring the standards used for intercepting e-mail messages up to the stricter, more protective level now applied to telephone wiretaps. Illegal interception of e-mail would result in suppression of the evidence, as is the case now with illegal interception of phone calls. The proposal would also enforce the same legal standards that apply to phone calls for interception of e-mails sent by cable modems, which have a greater degree of privacy protection under a law that governs cable systems.

The administration is also calling for greater authority for courts to review law enforcement requests to use devices that record the phone numbers of incoming and outgoing calls and to track the origins and destinations of e-mail messages.

These changes are clearly needed. But Congress also needs to provide new safeguards against the government's wrongful use of ever more powerful surveillance technology against law-abiding citizens. Serious concerns have been raised about Carnivore, the new online wiretap system used by the F.B.I. to track the communications of individuals suspected of criminal activity.

The F.B.I. says the technology can isolate the e-mail of the target of an investigation. But the system, when hooked up to the network of the Internet service provider, gives the F.B.I. unlimited access to the e-mail of all other subscribers on the network. While a court order is still required to intercept the content of messages, the secret technology controlled exclusively by law enforcement raises fears of improper monitoring.

Until now, routine government surveillance of private conversations was limited as much by practicality as by legal constraints. Now that it is feasible to eavesdrop electronically on an unlimited scale, the laws have to be strengthened to prevent monitoring of all online communications simply because technology makes it easy.

5/24/02 Release - Page 15
Doc. # 24

The Washington Times

DATE: 7-28-00

PAGE: A-20

The warning from Colombia's Serrano

Since the United States approved $1.3 billion in counternarcotics aid for Colombia, guerrilla groups who profit from the drug trade have waged a bloody terror campaign in protest. Even as Colombian government officials and guerrilla leaders sat around a peace table in Geneva on Monday and Tuesday, the bloodshed in Colombia continued unabated.

Since January, when aid to Colombia was approved, the Revolutionary Armed Forces of Colombia (FARC), a guerrilla group, has attacked almost 200 police stations and killed more than 100 police officers. Fighting that began over the weekend in Colombia's northern San Lucas mountains appears to have resulted in the deaths of 60 members of the National Liberation Army (ELN) guerrilla group and 18 renegade, paramilitary fighters. In addition, on Monday 200 FARC terrorists ambushed a police station in the remote southwestern province of Narino, which is rich in opium poppy fields. The FARC gunned down 11 police officers and wounded 17 others.

This summit's context of violence highlights how brutal guerrilla and paramilitary tactics continue to be. Commanders for the FARC, which has effective control of about 40 percent of the country, declined even to attend the summit. But the relatives of 11 people kidnapped by the ELN in the spring of 1999 were there, lobbying for the release of their loved ones. The ELN's chief, Antonio Garcia, gave them little hope, pre-empting the summit by saying that neither the issue of hostages nor a cease-fire would be on the table for discussion.

What the ELN did want to discuss is the 1,500 square-mile territory that Colombian President Andres Pastrana has tentatively agreed to surrender to ELN control. But the agreement is difficult to implement since the area, which is rich in oil, gold and cocaine, is overrun by paramilitary forces.

In addition, local residents are strongly opposed to forfeiting the region to the ELN, since they fear living outside of the government's protection. The government gave the FARC control of a demilitarized zone about one year ago and an ombudsman appointed by Congress has documented 41 disappearances in the territory at the hands of the FARC. The territory was ceded as a land for peace deal, but the FARC now uses the demilitarized zone as a base of illegal operations and has shown no will whatsoever to negotiate a peace.

Former Colombian Police Chief Jose Serrano, who was in Washington last week to receive the DEA's special agent award, described the growing link guerrilla and paramilitary groups have formed with drug traffickers, giving terrorists access to vast resources to buy guns. "After the iron curtain fell, and subversives stopped receiving money from the former Soviet Union or Cuba, the FARC began attacking us when we fumigated [coca] crops," Mr. Serrano told The Washington Times. Mr. Pastrana's plan to achieve peace through counternarcotics initiatives and social projects is therefore "the last chance that we Colombians have. Because if it fails, we will have to make our peace over corpses," he said. No one should want that. Colombia has seen enough suffering.

17

Los Angeles Times

DATE: 2-27-00
PAGE: A-15

Who Needs Big Brother When There's 'Carnivore'?

■ Law enforcement: The FBI should not be granted such sweeping powers to search our e-mail and then be trusted to police itself.

By BART KOSKO

Now the FBI wants to recruit Internet service providers, or ISPs, to spy on U.S. citizens. The FBI already works with the credit companies to secretly snoop on large portions of our digital credit reports per the 1996 Intelligence Authorization Act. The FBI has installed digital phone-tapping equipment directly in phone companies under a similar congressional act passed in 1994. And the Treasury Department's Financial Crimes Enforcement Network has "deputized" all banks to monitor our bank accounts and to secretly file "suspicious activity reports" that it shares with the FBI and IRS and even with some foreign governments.

The FBI calls its new ISP surveillance software "Carnivore." An agent connects a laptop to the ISP server and then reads at least the address of every e-mail message that passes through the server. The FBI says it has used its Carnivore software 25 times in the last two years to search for terrorists or drug dealers or child pornographers. The FBI claims that it needs this search-'em-all software to help it find and catch such criminals when they use the Internet.

There are three problems with Carnivore, and each is fatal. The first is that Carnivore undermines the 4th Amendment's ban on unreasonable searches—if it does not violate it outright. The FBI still must get a judge to issue a search warrant based on "probable cause." This in practice can mean no more than that the FBI asks for the warrant. But the 4th Amendment further demands that the warrant be specific—"particularly describing the place to be searched."

Carnivore searches blindly through all private e-mails that flow through the ISP server while it looks for a suspicious few. This is as if the police have a warrant to search someone's bedroom closet and then search all houses in a city until they find it. The search itself invades privacy.

Carnivore switches the order of search and identification. Traditional searches first identify the suspect's property, which is then searched. Carnivore searches through private databases until it identifies a suspect's property—and perhaps learns some new things along the way. This is a big leap down the slippery slope of state invasion of privacy. And the very existence of such a monitoring system produces a chilling effect on e-mail-based free speech, because knowing that a state police agency will read at least part of your e-mail message affects what you say in that message.

The second problem is that the FBI does not need Carnivore to search for alleged criminal e-mails. Rep. John Conyers Jr. (D-Mich.) raised this issue with FBI Assistant Director Donald Kerr when Kerr testified before Congress at a hearing Monday on Carnivore: "Why do we need to put terminals on site at the ISPs rather than let the ISP itself turn over needed information much in the way that telephone companies do?"

Kerr conceded this point but claimed that the FBI still needs Carnivore for those ISPs that lack filtering software. This is plainly specious: The FBI or oversight sources could simply give such ISPs this filtering software. There is simply no need to grant the FBI such sweeping powers of search and then trust the agency to police itself as those powers inevitably grow in time.

The third problem is that Carnivore ultimately will not work despite all its costs. The criminals it tries to watch are the very people who will take the two obvious steps to evade it: They will change their fake digital IDs more often, and they will use ever more powerful digital encryption to scramble their messages.

Carnivore's software blueprints and performance quirks themselves will leak to the digital underground despite or because of the best efforts of those in Congress or the judiciary who oversee it. And hackers will surely study the software system and maybe crack it.

The only people Carnivore can confidently watch are the innocent citizens whom it has no right to watch. This sets a foolish and dangerous precedent for the type of heavy-handed government surveillance one would expect to find in Myanmar or China.

The only thing right about Carnivore is its name: This digital beast devours both personal privacy and constitutional limits on state police power. Congress should kill it.

Bart Kosko is a professor of electrical engineering at USC and the author of "The Fuzzy Future" (Random House, 1999).

18

Doc. #26

The New York Times

DATE: 7-27-02

PAGE: C2

Microsoft Files Brief Asking Supreme Court to Send Antitrust Case to Appeals Court

By STEVE LOHR

In a legal document filed yesterday, Microsoft argued that the government's antitrust case is "completely unsuitable for direct appeal" to the Supreme Court because it is complex and because the trial judge made "serious and substantive procedural errors."

Microsoft wants its appeal to go first to the federal appeals court in Washington, which ruled in favor of the company in a related case.

The company's argument, filed with the Supreme Court, rests heavily on a scathing attack on the work of Judge Thomas Penfield Jackson, who heard the lawsuit in Federal District Court.

The Microsoft document, citing interviews Judge Jackson granted to new organizations, including The New York Times, stated, "The district court's blunt comments to the press raise serious questions about its impartiality."

Microsoft also questioned the even-handedness of Judge Jackson's decisions in general. First, the company asserted, the judge improperly allowed the Justice Department and 19 states suing the company to broaden their case. Then, after allowing the additional evidence, Judge Jackson assured the company that his findings would be based on the more limited, original complaint, according to the Microsoft filing.

Those "assurances," the company stated, "the district court would later repudiate."

Judge Jackson ruled earlier this year that Microsoft was a monopolist that had repeatedly violated antitrust laws, and he ordered that the company be split in two — an order he later shelved pending appeals.

If the case goes straight to the Supreme Court, it could be resolved in a year. If it goes first to the appeals court, the resolution might take up to two years.

The government is seeking to have the Supreme Court hear the appeal directly and sidestep a review by a federal appeals court. Direct appeals to the court are permitted in major antitrust cases brought by the government. Four of the nine justices must vote in favor for the case to go directly from the district court.

In its filing, Microsoft is trying to persuade the court that the appeal will involve a thicket of technical issues, procedural challenges and disputed facts. Sorting out these matters, Microsoft says, will involve poring over the voluminous written record of the lengthy trial – precisely the kind of winnowing usually left to an appeals court. The Justice Department had no comment yesterday, other than a brief statement saying that the government "will respond in its filing."

The software company says the trial judge made procedural errors.

Still, there is little mystery about what the government's theme will probably be when it files its brief with the court on Aug. 15. First, according to legal experts, the government will say that the factual findings are clear and that the issues for appeal are a couple of big legal questions — precisely the kind of major judgments of law that the court so often reserves for itself.

The big legal issues, they say, are whether Microsoft's bundling of its Internet browser with its industry-standard Windows operating system was an illegal tying of two products and whether Microsoft's dealings with other companies was indeed "monopolizing conduct," in legal parlance. Judge Jackson ruled that Microsoft's bundling move and its behavior did violate antitrust laws, and Microsoft is appealing his ruling.

The government is also expected to make a forceful policy argument for the expedited appeal, given the importance of computer industry to the economy.

"The government will say that Microsoft's monopoly is imposing a significant social cost while this case is on appeal and no remedies are in place," said Herbert Hovenkamp, a professor at the University of Iowa law school. "It will say that not taking the case is a costly act, and that this is exactly the kind of case that was meant to go directly to the Supreme Court."

In its 30-page filing, Microsoft stated that the case "went badly awry from the outset," referring to Judge Jackson's decision to permit the government to add additional evidence after the suit was filed in May 1998.

That move, Microsoft said, allowed the Justice Department and states to "transform their case beyond recognition." In doing so, Microsoft declared that the judge "committed an array of serious and substantive procedural errors."

These errors, Microsoft said, included giving the company too little time for discovery and preparation of its defense to the expanding array of evidence.

Much of the evidence in the case, Microsoft contends, should have been tossed aside as not being suitable for admission in court. "The district court," Microsoft stated, "largely suspended application of the federal rules of evidence, admitting numerous newspaper and magazine articles and other rank hearsay."

Judge Jackson, legal analysts say, did allow a wide range of written evidence in the case. But he gave that leeway to both sides, they said, noting that Microsoft submitted many newspaper articles, even press releases, as evidence.

And the government maintained that the additional evidence presented after the complaint was filed was part of the "pattern" of anticompetitive practices Microsoft used to stifle competition. Thus, the government said, the additional evidence involving companies like Intel and Apple was not an expansion of the original complaint, but merely further examples that fit the same pattern of behavior. Judge Jackson agreed with the government.

In its filing, Microsoft suggested that in its appeal, the company will seek to make sure that it no longer appears before Judge Jackson. It said his comments to the press should be considered grounds for a

19

Doc. #27 cont'd

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF GENERAL COUNSEL
TECHNOLOGY LAW UNIT
(THROUGH 7/28/00)

PAGES REVIEWED: 49

PAGES RELEASED: 49

EXEMPTIONS CITED: b6-1, b7C-1, b6-3 & b7C-3

NOTE: 91 pages from this file are duplicates to pages from The Office of General Counsel's Front Office file.

In Congress
American Civil Liberties Union
Freedom Network

July 11, 2000

VIA FAX
Hon. Charles T. Canady, Chairman
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

and

Hon. Melvin L. Watt, Ranking Member
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

Dear Representatives Canady and Watt:

We are writing to you about the new FBI email surveillance system aptly named "Carnivore," which gives law enforcement extraordinary power to intercept and analyze huge volumes of email. The Carnivore system gives law enforcement email interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act (ECPA), codified in relevant part at 18 U.S.C. 2510-22 and 18 USC 3121-27. Carnivore raises new legal issues that cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age.

The existence of Carnivore first came to light in the April 6 testimony of Attorney Robert Corn-Revere to the Constitution Subcommittee. Its operation was further detailed in a report that appeared in today's Wall Street Journal (copy attached). According to these reports, the Carnivore system -- essentially a computer running specialized software-- is attached directly to an Internet Service Provider's (ISP) network. Carnivore is attached either when law enforcement has a Title III order from a court permitting it to intercept in real time the contents of the electronic communications of a specific individual, or a trap and trace or pen register order allowing to it obtain the "numbers" related to communications from or to a specified target.

But unlike the operation of a traditional a pen register, trap and trace device, or wiretap of a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP's network, not just the communications to or from a particular target. Carnivore, which is capable of analyzing millions of messages per second, purportedly retains only the messages of the specified target, although this process takes place without scrutiny of either the ISP or a court.

Carnivore permits access to the email of every customer of an ISP and the email of every person who communicates with them. Carnivore is roughly equivalent to a wiretap capable of

accessing the contents of the conversations of all of the phone company's customers, with the "assurance" that the FBI will record only conversations of the specified target. This "trust us, we are the Government" approach is the antithesis of the procedures required under our the wiretapping laws. They authorize limited electronic surveillance of the communications of specified persons, usually conducted by means of specified communications devices. They place on the provider of the communications medium the responsibility to separate the communications of persons authorized to be intercepted from other communications.

Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. Carnivore is not a minimization tool. Instead, Carnivore maximizes law enforcement access to the communications of non-targets.

In his testimony to your subcommittee Mr. Corn-Revere described the experience of his client, an ISP that was required to install Carnivore when presented with a trap and trace order. He detailed his client's concerns that a trap and trace order in the context of the Internet revealed information that Congress did not contemplate when it authorized their limited use. In the traditional telephone context, those orders reveal nothing more than the numbers dialed to or from a single telephone line. In the Internet context, these orders and certainly Carnivore, likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication.

As we have stated previously, the ACLU does not believe that it is clear that the Government can serve an order on an Internet service provider and obtain the e-mail addresses of incoming and outgoing messages for a particular subscriber. Further, it is not clear whether law enforcement agents use or should use authority under the pen register statute to access a variety of data, including Internet Protocol addresses, dialup numbers and e-mail logs. We certainly do not believe that it is clear that law enforcement can install a super trap and trace device that access to such information for all of an ISP's subscribers.

In light of the new revelations about Carnivore, the ACLU urges the Subcommittee to accelerate its consideration of the application of the 4th Amendment in the digital age. Legislation should make it clear that law enforcement agents may not use devices that allow access to electronic communications involving only persons other than a specified target for which it has a proper order. Such legislation should make clear that a trap and trace order served on an ISP does not authorize access to the contents of any communication - including the subject line of a communication -- and that the ISP bears the burden of protecting the privacy of communications to which FBI access has not been granted.

We would be happy to work with the Subcommittee on drafting legislation that protects the privacy rights of Americans.

Sincerely,

Laura W. Murphy
Director, ACLU Washington National Office

Barry Steinhardt
Associate Director, ACLU

Gregory T. Nojeim

Legislative Counsel, ACLU Washington National Office

cc: Members of the Constitution Subcommittee of the House Judiciary Committee

[Legislative Archives] [106th Congress Issues] [Voters' Guide] [Congress Overview] [How to Use this Section]
INDEX | JOIN | HOME | SEARCH | FEEDBACK

Copyright 1999, The American Civil Liberties Union

Want to send this story to another AOL member? Click on the heart at the top of this window.

Stronger Online Privacy Sought

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - Lawmakers are seeking ways to shore up online privacy following reports of businesses selling customers' personal information and an FBI system that hunts for suspects by scanning citizens' e-mail.

Sens. Patrick Leahy, D-Vt., and Robert Torricelli, D-N.J., introduced legislation that would bar the sale of personal information kept by a defunct company if the sale would have violated privacy policies in effect when the company was in business.

The bill responds to the case of Toysmart, a former online toy retailer that put all its assets, including its customer records - such as names, addresses and credit card numbers - up for sale despite a privacy policy that assured customers the information would remain private.

The Federal Trade Commission filed a suit against Toysmart this week to stop the sale from taking place. Rep. Spencer Bachus, R-Ala., has already announced plans to introduce a similar bill in the House.

"It is wrong to use our nation's bankruptcy laws as an excuse to violate a customer's personal privacy," the senators said in a letter to colleagues asking for support for the bill. "Customers have a right to expect a firm to adhere to its privacy policies, whether it is making a profit or has filed for bankruptcy."

The legislators say they will try to include the bill in a larger bankruptcy reform package.

TRUSTe, an organization that gives its seal to Web sites that meet its privacy principles, blew the whistle on Toysmart in June.

Earlier Wednesday, Walt Disney, the majority owner of Toysmart, said it has offered to purchase the company's lists and assure their confidentiality.

In a related action, two legislators are going after "Carnivore," a system in use by the FBI to monitor suspected criminals' e-mail. Carnivore is installed at a suspect's Internet provider and scans through all incoming and outgoing mail, looking for messages belonging to the suspect.

Privacy groups, such as the American Civil Liberties Union and the Electronic Information Privacy Center, and some Internet providers object to the system because Internet companies have no control over the "black box." They say it infringes upon the rights of individuals not involved with the FBI investigation.

The ACLU sent a letter to Rep. Charles Canady, R-Fla., detailing its concerns. Canady will announce Thursday the date for hearings on Carnivore, his spokesman said.

House Majority Leader Dick Armey sent a letter Wednesday to Attorney General Janet Reno and FBI Director Louis Freeh blasting the agencies and the Clinton administration for the "cybersnooping" system.

"The federal government has the power and the authority to collect and maintain vast amounts of private personal information," wrote Armey, R-Texas. "This administration continues to demonstrate a cavalier attitude with that responsibility."

Also, Rep. Clay Shaw, R-Fla., will introduce a bill Thursday aimed at stopping identity theft. The bill would prohibit the sale of Social Security numbers, which can be used to get credit card numbers, bank loans and accounts in another person's name. The FTC announced Wednesday that calls to their identity theft hot line are on the rise, at about 850 reports per week.

"Identity theft is a terrible problem that has literally destroyed people's lives and it must be stopped," said Shaw, who heads the House Social Security subcommittee.

On the Net: TRUSTe: http://www.truste.org

F2

American Civil Liberties Union: http://www.aclu.org

Privacy International: http://www.privacy.org/pi/

AP-NY-07-12-00 1915EDT

Copyright 2000 The Associated Press. The information contained in the AP news report may not be published, broadcast, rewritten or otherwise distributed without the prior written authority of The Associated Press. All active hyperlinks have been inserted by AOL.

FBI Cybersnooping System Raises Additional Privacy Concerns

Armey to Administration: Stay Out of My Inbox!

July 12, 2000



Related Links

The e-Contract

Remarks on the e-Contract with High Tech America

FBI Cybersnooping System Raises Privacy Concerns

Only Violate Personal Privacy in the Right Way?

Is the Government in a Position to Talk About Internet Privacy?

House Majority Leader Dick Armey today called on Attorney General Janet Reno and FBI Director Louis Freeh to address the privacy concerns raised by the Federal Bureau of Investigation's Carnivore system of monitoring email traffic. Armey issued the following statement:

This Administration doesn't have the best record on personal privacy. It keeps repeating the same mistake over and over.

Last year, a draft Administration proposal for a computer network monitoring system called FIDNet surfaced. When I joined privacy advocates in questioning the legitimacy of a government system that could monitor *private sector* networks, the Administration backed off a bit from their original design. But it has yet to answer my question of why they intended to monitor private systems in the first place.

Now the FBI wants to run a system that could sort through every single e-mail message that passes through a commercial Internet service provider. I ask, why should we trust this Administration with our most personal correspondence?

At a time when there is a lot of talk about concerns for Internet privacy, the Clinton-Gore Administration continues to push Big Brother proposals that promote government cybersnooping. They seem tone deaf to the concerns people have about the government invading their privacy. The Federal government has the power and the authority to collect and maintain vast amounts of private personal information. This Administration continues to demonstrate a cavalier attitude with that responsibility.

I call on Attorney General Reno and FBI Director Freeh to stop using this cybersnooping system until fourth amendment concerns are adequately addressed.

Related Correspondence:

- First letter to AG Reno
- Second letter to AG Reno
- Third letter to AG Reno
- Privacy violations at ONDCP
- Letter to the president on web privacy

- Letter to the IRS on privacy violations





The Nation's communications networks are routinely used in the commission of serious criminal activities, including espionage. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities.

The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence -- not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,600 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques.

In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. This type of tool is necessary to meet the stringent requirements of the federal wiretapping statutes.

The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being

transmitted either to or from the named subject.

Carnivore serves to limit the messages viewable by human eyes to those which are strictly included within the court order. ISP knowledge and assistance, as directed by court order, is required to install the device.

The use of the Carnivore system by the FBI is subject to intense oversight from internal FBI controls, the U. S. Department of Justice (both at a Headquarters level and at a U.S. Attorney's Office level), and by the Court. There are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties. The system is not susceptible to abuse because it requires expertise to install and operate, and such operations are conducted, as required in the court orders, with close cooperation with the ISPs.

The FBI is sharing information regarding Carnivore with industry at this time to assist them in their efforts to develop open standards for complying with wiretap requirements. The FBI did so two weeks ago, at the request of the Communications Assistance for Law Enforcement Act (CALEA) Implementation Section, at an industry standards meeting (the Joint Experts Meeting) which was set up in response to an FCC suggestion to develop standards for Internet interception.

This is a matter of employing new technology to lawfully obtain important information while providing enhanced privacy protection.

| Programs and Initiatives | FBI Home Page |

b6-1 / b7c-1

From: [redacted] b6/b7c-1
To: KERR, DONALD
Date: Tuesday, July 18, 2000 9:24PM
Subject: CARNIVORE BRIEFING FOR DAG 2PM 7/19

Dr. Kerr, b6-3/b7c-3

I received a call this evening from [redacted] relaying a request from the DAG's Office that you and [redacted] be available for a briefing of Deputy Attorney General Eric Holder tomorrow in Mr. Holder's Conference Room (room 4111) at DOJ at 2:00 PM. [redacted] b6-3/b7c-3 requested my presence as well. [redacted] was previously scheduled to brief DOJ at 12:30. I have contacted him and he has confirmed that the briefing has been rescheduled for 2:00 PM and will now include the DAG. I will have to come back in from CART at Fredericksburg, or another representative of OGC will be present.

b6-1/b7c-1

b6-1/b7c-1

We have been asked to confirm our attendance by contacting [redacted] at [redacted] b6-3/b7c-3

[redacted]
Technology Law Unit
Office of the General Counsel
FEDERAL BUREAU OF INVESTIGATION
935 Pennsylvania Ave., N.W. Rm [redacted]
Washington, D.C. 20535-0001
Tel [redacted]
Fax [redacted]
Pag [redacted]
No Internet E-Mail Address

b6-1
b7c-1

CC: [redacted] b6-1 b7c-1

Doc. #5

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc #4, OGC Front Office Docs., Wall Street Journal Article (7/14/04) (Page 4)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #6 (Page 165)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

14 Pages were not considered for release as they are duplicative of Doc #13 pgs. 1-14 OGC FRONT OFFICE FILE (pgs. 20-33)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
Doc #8 (Pages 167-180)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

6C-1
67C-1

From: [redacted]
To: CHARLES STEELE, [redacted]
Date: 7/21/00 5:48PM
Subject: Latest version

Charlie [redacted]

Attached is a copy of the statement with the DOJ revisions having been made.

DOC. # 9

66-1 / 67C-1

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the FBI's Internet and data interception capabilities and to help set the record straight regarding this important issue. I would like to first discuss the FBI's legal authority for conducting interceptions on the Internet, and then describe the technical means by which we intercept Internet communications in order to obtain evidence of Federal felonies.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting a part of our interception software - codenamed Carnivore as an ominous new technology that raised concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that our statutory law enforcement authorities be discussed openly. In fact, this was the reason we chose to share information about this capability with industry experts several weeks ago. As technology continues its rapid evolution, it is essential for the public to know and understand their government is scrupulously observing the laws and the constitutional protections that guarantee their right to privacy. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our capabilities are used only after lawful court ordered authorization and that they are directed at the most serious violations of national security and public safety.

66-1 / 67C-1

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), which is commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". All such interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated. Last year, the FBI obtained Title III court orders in 327 instances. We did not initiate surveillances under emergency provisions of Title III.

Federal surveillance laws supplement the Fourth Amendment's dictates concerning reasonable searches and seizures to oral, wire and electronic communications. They also include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects.

An application for a warrant to search a private residence must be presented under oath to a judge or magistrate who may issue the warrant only upon a finding of probable cause to believe that a crime has been committed, and that specified evidence of the crime will be found in the place to be searched. Applications for Title III interceptions of wire, oral or electronic communications must be presented to judges in the same way (magistrates are not authorized to approve Title III applications). However, before the application can even be submitted to the court, it must be authorized by a senior official of the Department of Justice (DOJ). Title III requires such high-level approval for applications to intercept oral and wire communications, except in the case of digital pagers, and DOJ policy requires the same level of approval for applications to intercept

66-1/67C-1

electronic communications, even though the law would allow lower-level approval.

Applications for electronic surveillance describe with particularity and specificity the particular offenses being committed, the communications facility or place from which the subject's communications are to be intercepted, a description of the types of communications to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Under Title III, electronic surveillance for criminal investigations is permitted only for the purpose of gathering hard evidence-- not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are obtained. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

66-1 / 67C-1

Within a reasonable period of time after the termination of the interception order, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory that includes notice of the order, the dates during which the interceptions were carried out, and whether or not the communications were intercepted. Upon motion, the judge may also direct that portions of the contents of the intercepted communication be made available to affected persons for their inspection.

A variety of sanctions are available to penalize interceptions conducted in violation of Title III, ECPA and the Fourth Amendment. The evidence obtained through such unlawful interceptions can be suppressed. The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, may recover in a civil action against the person or entity engaged in the violation, damages, including punitive damages, attorney's fees and other costs.

Once we obtain an order for surveillance of wire communications, we generally require technical assistance from the carrier or service provider. Such help is increasingly necessary the case with the advent of advanced communications services and networks such as the Internet. The days of connecting a pair of allegator clips connecting a tape recorder to a copper wire phone are long gone. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders. Upon the request of the applicant, a court order authorizing the interception of communications may direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted."

6C-1/67C-1

In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. The prohibition on using or disclosing the contents of communications illegally intercepted, likewise extends to service providers and their personnel. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in most cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue orders for Title III interceptions more narrowly tailored than those in the early years of Title III existence that were directed against "plain old telephone services." To be successfully implemented, these orders require complex methods to ensure that only messages for which there is probable cause to intercept are, in fact, intercepted. The increased detail in court orders issued under Title III responds to two relatively recent developments.

First, the complexity of modern communications networks, such as the Internet, and the complexity of modern users' communications equipment require better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services,

66-1 / 67C-1

like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has probable cause, to the exclusion of all others, very difficult. Court orders therefore increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program that is known as "Carnivore." The committee may be aware that Internet transmissions are broken down into packets of information consisting of a string of words or symbols. Different packets from the same message often take different routes between the sender and the intended recipient. The various packets constituting a single message are labeled so that they can be reassembled and read by the recipient. The challenge for law enforcement implementing a court order for interception of E-mail is to find and retrieve only those packets that are part of a message covered by the order. To do this, we developed a software solution to perform network analysis. This software runs on a standard personal computer running the standard Microsoft Windows operating system. It works by " sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programed in conformity with the court order. This filter set can be extremely complex, but it provides the FBI with an ability to collect only those transmissions which comply with pen register court orders, trap & trace court orders, and Title III interception orders.

66-1/67C-4

It is important to understand what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what our software does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use this program at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how we use the system in practice. First, there is the issue of scale. Carnivore is a small-scale tool intended for use only when and where it is needed. In fact, each one is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is

6C-1 / 67C-1

connected by a high impedance bridge and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, it is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This leads to the third issue--that of ISP cooperation. To my knowledge, we have never installed this system onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be difficult, if not impossible, for law enforcement agencies to successfully implement and comply with the strict language of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using this system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires the authentication of evidence as a condition of its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices without lawful authorization from a court. Over the last five years or more, we have witnessed a continuing, steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities that have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively

b6-1 / b7c-

investigate and prevent these crimes is, in part, dependant upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software.

I look forward to working with the subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank You.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

76 Pages were not considered for release as they are duplicative of DOCUMENT #14, OGC FRONT OFFICE FILE (PAGES 45-120)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #10 (PAGES 191-266)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

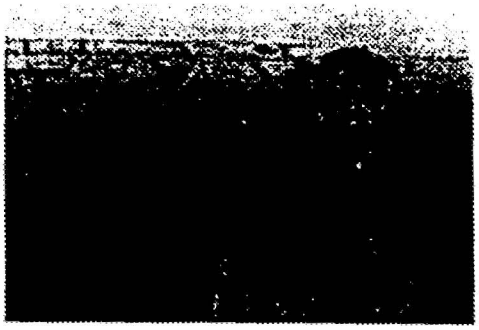
XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Alan Davidson

Staff Counsel

abd@cdt.org Recent Presentations



Alan Davidson is Staff Counsel at the Center for Democracy and Technology (CDT), a Washington D.C. non-profit group working to promote civil liberties on the Internet and other new digital media. Mr. Davidson is currently leading CDT's efforts to promote encryption policies that protect privacy and free expression in the information infrastructure. He has written and spoken widely on the civil liberties implications of public policies that restrict encryption, and has been directly involved in the ongoing Congressional debate over cryptography legislation.

Mr. Davidson also works more broadly on issues relating to Internet policy including free speech and censorship, Internet governance, digital signatures and electronic commerce, domain name issues, and online gaming. He took part in CDT's coordination of one of the two victorious challenges to the Communications Decency Act at the Supreme Court in ACLU v. Reno. His other research interests lie generally in the areas of privacy, free speech, and the special problems posed by the interaction of technology, public policy, and the law.

Mr. Davidson was a computer scientist before joining the legal profession. His earliest hacker credentials came as the proud owner of a Commodore PET in the late 1970s. A graduate of the Massachusetts Institute of Technology, he received an S.B. in Mathematics and Computer Science and later returned for an S.M. in Technology and Policy. Mr. Davidson worked as a Senior Consultant at Booz-Allen & Hamilton, designing the information systems for NASA's Space Station Freedom Project. He has also worked on technology and policy issues at the U.S. Congress Office of Technology Assessment and for the White House Office of Policy Development Health Care Task Force.

Mr. Davidson attended law school at Yale, where he was Symposium Editor of the Yale Law Journal. He remains active in MIT alumni affairs, and recently completed a 4-year term as a Trustee of the MIT Corporation. He also enjoys backpacking, skiing, and is currently learning to speak Spanish.

©2000 The Center For Democracy & Technology
1634 Eye Street NW, Suite 1100
Washington, DC 20006
(v) 202.637.9800
(f) 202.637.0968
Technical concerns about this site: webmaster@cdt.org
Concerns or opinions about issues: feedback@cdt.org

News
American Civil Liberties Union
Freedom Network

In Unique Tactic, ACLU Seeks FBI Computer Code On "Carnivore" and Other Cybersnoop Programs

FOR IMMEDIATE RELEASE
Friday, July 14, 2000

WASHINGTON -- In what may be the first request of its kind, the American Civil Liberties Union is asking the Federal Bureau of Investigation to disclose the computer source code and other technical details about its new Internet wiretapping programs.

In a Freedom of Information Act (FOIA) request sent today to the FBI, the ACLU is seeking all agency records related to the government e-mail "cybersnoop" programs dubbed Carnivore, Omnivore and Etherpeek, including "letters, correspondence, tape recordings, notes, data, memoranda, email, computer source and object code, technical manuals, [and] technical specifications."

Computer "source code" is the set of instructions for a program written by its creators, which is compiled into "object code" which can be read by machines.

"Right now, the FBI is running this software out of a black box," said Barry Steinhardt, Associate Director of the ACLU and author of the letter. "The FBI is saying, 'trust us, we're not violating anybody's privacy.' With all due respect, we'd like to determine that for ourselves."

To the ACLU's knowledge, the request for program source code is the first of its kind. But Steinhardt said that two federal appeals court rulings that computer code is a form of speech, no different from any other written document, support the ACLU's demand under the the Freedom of Information Act. The Act gives Americans broad rights to obtain written information held by the federal government.

Technical data on traditional telephone wiretaps is currently available in public documents, Steinhardt said. Similar access to the computer source code of Carnivore and other such programs is necessary to determine just how the software operates and whether e-mail privacy is being violated.

The unbridled uses of these technologies "cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age,"the ACLU said in a July 11 letter to members of Congress.

Revelations about the Carnivore program also prompted calls for disclosure from lawmakers concerned about privacy. In a statement issued on July 12, House Majority Leader Dick Armey called on Attorney General Janet Reno and FBI Director Louis Freeh to "stop using this cybersnooping system until Fourth Amendment concerns are adequately addressed."

In addition, the House Judiciary Committee Subcommittee on the Constitution has scheduled a hearing on the matter for Monday, July 24. The ACLU has asked to submit testimony to the Committee.

The FBI has 20 business days to respond to the FOIA request. The ACLU is seeking a response on an expedited basis, the letter said, "because this information relates to impending policy decisions to which informed members of the public might contribute."

"If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the act," the ACLU letter concluded.

The ACLU's letter to the FBI follows.

July 14, 2000

Attention:
John Kelso Jr.
Federal Bureau of Investigation
Chief, FOI/PA Section, Rm. 6296 JEH
Washington, D.C. 20535-0001

Dear Mr. Kelso:

We are writing pursuant to the Freedom of Information Act (5 U.S.C. Sec. 552) to request all agency records including letters, correspondence, tape recordings, notes, data, memoranda, email, computer source and object code, technical manuals, technical specifications, or any other materials held by the Federal Bureau of Investigation regarding the following:

1. The computer system, software or device known as "Carnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers;

2. The computer system, software or device known as "Omnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers, and

3. The computer system, software or device known as "EtherPeek", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers.

We seek a waiver of fees associated with the fulfillment of this request for all search and processing fees, pursuant to Section 552(a)(4)(A)(ii)(II) of the Freedom of Information Act. Records are not sought for commercial use, and as a representative of the news media, the American Civil Liberties Foundation (ACLU Foundation) qualifies for a fee waiver under this provision of the FOIA. The organization meets the criterion laid out in National Security Archive v. Department of Defense, where a representative of the news media is defined as an entity that "gathers information of potential interest to a segment of the public" and "uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." 881 F. 2d at 1387. The ACLU Foundation publishes newsletters, frequent press releases, news briefings, right to know handbooks, and other materials that are disseminated to the public. Its material is widely available to everyone including tax exempt organizations, not-for-profit groups, law students and faculty for no cost or for a nominal fee through its public education department. The ACLU Foundation disseminates information through publications available on-line at www.aclu.org as well.

In addition we request a fee waiver for duplication costs because disclosure of this information is in the public interest. It is likely to contribute significantly to the public understanding of the activities of the government. The ACLU Foundation is a nonprofit

501(c)3 research and education organization working to increase citizen participation in governance issues. The ACLU Foundation is making this request specifically for the public's enhanced understanding of lawfully authorized wiretapping, its relationship to constitutional guarantees of privacy as well as an understanding of global technological developments in wire and electronic networks that facilitate and expedite such wiretapping. The public's interest is particularly pertinent in light of advancing communications technology and the rapid growth of the World Wide Web. These developments have greatly increased the communications interconnectedness of all the countries in the world, especially technologically advanced nations like the US and the Netherlands.

We also seek expedited review of this FOIA request because this information relates to impending policy decisions to which informed members of the public might contribute. Timely public access to these materials is necessary to fully inform the public about the issues surrounding communications interception and related technological developments.

If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the act. We expect you to release all segregable portions of otherwise exempt material. We reserve the right to appeal your decision to withhold any information or to deny a waiver of fees.

We look forward to your reply within 20 business days, as the statute requires under Section 552(a)(6)(A)(I).

Thank you for your assistance.

Sincerely,

Barry Steinhardt, Esq.
On behalf of the ACLU Foundation

INDEX | JOIN | HOME | SEARCH | FEEDBACK

Copyright 2000, The American Civil Liberties Union

News
American Civil Liberties Union
Freedom Network

ACLU Urges Congress to Put a Leash on "Carnivore" And Other Government Snoopware Programs

FOR IMMEDIATE RELEASE
Wednesday, July 12, 2000

WASHINGTON -- Law enforcement officials using new surveillance technologies online are racing far ahead of established privacy law and must be reined in, the American Civil Liberties Union said today.

In a letter sent to Charles T. Canady, R-FL, Chair of the Constitution Subcommittee of the House Judiciary Committee, and ranking member Melvin L. Watt, D-NC, the ACLU said that the unbridled uses of these technologies "cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age."

Specifically, the ACLU sharply criticized the FBI's new online wiretapping program, dubbed "Carnivore," that uses Internet Service Providers (ISPs) to intercept and analyze huge amounts of e-mail from suspects and non-suspects alike.

"It is high time that lawmakers put a leash on Carnivore and other government schemes that go way beyond what Congress authorized under the Electronic Communications Protection Act," said Laura W. Murphy, director of the ACLU's Washington National Office and an author of the letter.

Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. But Carnivore does just the opposite, Murphy said, by sweeping in e-mails from innocent Internet users as well as the targeted suspect.

Barry Steinhardt, Associate Director of the ACLU and an author of the letter, said that implementing Carnivore "is comparable to allowing government agents to rip open Post Office mailbags and scan every piece of mail in search of one specific letter whose address they already know."

He also noted that while the system is plugged into the ISP, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

The snoopware program first came to light during an April 6 hearing before the Constitution Subcommittee. The Carnivore system -- essentially a computer running specialized software-- is attached either when law enforcement has a court order permitting it to intercept in "real time" the contents of the electronic communications of a specific individual, or a trap-and-trace or pen register order allowing to it obtain the numbers related to communications from or to a specified target.

But "in the Internet context," the ACLU letter said, "these orders and certainly Carnivore likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication."

In urging Congress to accelerate its consideration of applying Fourth Amendment principles in the digital age, "we would be happy to work with the Subcommittee on drafting legislation that protects the privacy rights of Americans," the ACLU letter said.

The letter was signed by Murphy, Steinhardt, and Gregory T. Nojeim, legislative counsel with the ACLU's Washington National Office, who testified at the April 6 hearing.

In recent related developments, the ACLU has criticized other government surveillance schemes, including a global electronic surveillance system -- known by the code name of "Echelon" -- that is capturing satellite, microwave, cellular and fiber-optic communications worldwide.

The ACLU's letter on Carnivore is online at: http://www.aclu.org/congress/l071100a.html.

For more information on the April 6 hearing, click http://www.aclu.org/news/2000/n040600b.html

For more information on "Echelon," go to http://www.aclu.org/echelonwatch/.

INDEX | JOIN | HOME | SEARCH | FEEDBACK

Copyright 2000, The American Civil Liberties Union



July 11, 2000

VIA FAX
Hon. Charles T. Canady, Chairman
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

and

Hon. Melvin L. Watt, Ranking Member
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

Dear Representatives Canady and Watt:

We are writing to you about the new FBI email surveillance system aptly named "Carnivore," which gives law enforcement extraordinary power to intercept and analyze huge volumes of email. The Carnivore system gives law enforcement email interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act (ECPA), codified in relevant part at 18 U.S.C. 2510-22 and 18 USC 3121-27. Carnivore raises new legal issues that cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age.

The existence of Carnivore first came to light in the April 6 testimony of Attorney Robert Corn-Revere to the Constitution Subcommittee. Its operation was further detailed in a report that appeared in today's Wall Street Journal (copy attached). According to these reports, the Carnivore system -- essentially a computer running specialized software-- is attached directly to an Internet Service Provider's (ISP) network. Carnivore is attached either when law enforcement has a Title III order from a court permitting it to intercept in real time the contents of the electronic communications of a specific individual, or a trap and trace or pen register order allowing to it obtain the "numbers" related to communications from or to a specified target.

But unlike the operation of a traditional a pen register, trap and trace device, or wiretap of a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP's network, not just the communications to or from a particular target. Carnivore, which is capable of analyzing millions of messages per second, purportedly retains only the messages of the specified target, although this process takes place without scrutiny of either the ISP or a court.

Carnivore permits access to the email of every customer of an ISP and the email of every person who communicates with them. Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the "assurance" that the FBI will record only conversations of the specified target. This "trust us, we are the Government" approach is the antithesis of the procedures required under our the wiretapping laws. They authorize limited electronic surveillance of the communications of specified persons, usually conducted by means of specified communications devices. They place on the provider of the communications medium the

responsibility to separate the communications of persons authorized to be intercepted from other communications.

Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. Carnivore is not a minimization tool. Instead, Carnivore maximizes law enforcement access to the communications of non-targets.

In his testimony to your subcommittee Mr. Corn-Revere described the experience of his client, an ISP that was required to install Carnivore when presented with a trap and trace order. He detailed his client's concerns that a trap and trace order in the context of the Internet revealed information that Congress did not contemplate when it authorized their limited use. In the traditional telephone context, those orders reveal nothing more than the numbers dialed to or from a single telephone line. In the Internet context, these orders and certainly Carnivore, likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication.

As we have stated previously, the ACLU does not believe that it is clear that the Government can serve an order on an Internet service provider and obtain the e-mail addresses of incoming and outgoing messages for a particular subscriber. Further, it is not clear whether law enforcement agents use or should use authority under the pen register statute to access a variety of data, including Internet Protocol addresses, dialup numbers and e-mail logs. We certainly do not believe that it is clear that law enforcement can install a super trap and trace device that access to such information for all of an ISP's subscribers.

In light of the new revelations about Carnivore, the ACLU urges the Subcommittee to accelerate its consideration of the application of the 4th Amendment in the digital age. Legislation should make it clear that law enforcement agents may not use devices that allow access to electronic communications involving only persons other than a specified target for which it has a proper order. Such legislation should make clear that a trap and trace order served on an ISP does not authorize access to the contents of any communication - including the subject line of a communication -- and that the ISP bears the burden of protecting the privacy of communications to which FBI access has not been granted.

We would be happy to work with the Subcommittee on drafting legislation that protects the privacy rights of Americans.

Sincerely,

Laura W. Murphy
Director, ACLU Washington National Office

Barry Steinhardt
Associate Director, ACLU

Gregory T. Nojeim
Legislative Counsel, ACLU Washington National Office

cc: Members of the Constitution Subcommittee of the House Judiciary Committee

Copyright 1999, The American Civil Liberties Union

Help | Contact Us | My Deja

Home >> Discussions >> alt.privacy.spyware

>> alt.privacy.spyware

>> Forum: alt.privacy.spyware
>> Thread: 'Carnivore' Won't Devour Cyber-Privacy
>> Message 11 of 1589

Save this thread
back to search results

deja.com Career Center
Powered by JobOptions.com
Explore More

Subject: Re: 'Carnivore' Won't Devour Cyber-Privacy
Date: 07/22/2000
Author: husky <cbminfo@digital.net>

<< previous in search · next in search >>

Message segment 2 of 2 - Get Previous Segment - Get All 2 Segments

If you give up your personal privacy, every other freedom will follow shortly. Though for my bucks, I say let carnivore loose. Whether carnivore does it's job or not has little to do with whether or not your health or credit records are safe. If you've posted your credit card anywhere on the web, chances are good it's no longer safe. And carnivore wouldn't have stopped that problem one way or the other. Health records ? Somehow I can't see hospitals storing personal patient records on the web, but maybe transmitting them for short periods to other computers but zero storage on the web.

> Fixing the relationship between Washington and Silicon Valley needs to
be
> a top priority for the next administration. The only people benefitting
from
> controversies like the one over Carnivore are terrorists, criminals and
> rogue states.

The above has little to do with carnivore the above mentioned groups will always exploit the weaknesses of others to gain their ends.
Carnivore is just the current subject under scrutiny.

Don't do your criminal activity over the web, and you haven't any reason to worry about carnivore. Couldn't get any simpler.

<< previous in search · next in search >>

Subscribe to alt.privacy.spyware
Mail this message to a friend
View original Usenet format
Create a custom link to this message from your own Web site

Search Discussions
Search only in
Search for
Search

DOC. #15

deja.com Before you buy

DO IT HERE JOB!

Help | Contact Us | My Deja

Home >> Discussions >> alt.comp.freewar

>> alt.comp.freeware

Power search SEARCH>>

>> Forum: alt.comp.freeware
>> Thread: British law would allow police to intercept e-mail
>> Message 2 of 1589

Save this thread

back to search results

Subject: Re: British law would allow police to intercept e-mail
Date: 07/24/2000
Author: TallesIn2 <tallesin2@earthlink.net>

POST REPLY

<< previous in search · next in search>>

Message segment 1 of 2 - Get Next Segment - Get All 2 Segments

URGENT ACTION ITEM! Congress agrees to hold
hearing on Monday in response to public outrage
over FBI's e-mail spy scheme
==========

==========

You are receiving this alert because you participated in DefendYourPrivacy.com's successful 1999 campaign against the FDIC's proposed Know Your Customer bank spying regulation. If you do not want to receive further updates, please use the unsubscribe directions at the end of this message.

==========

* Immediate action required: Help us Kill the
Carnivore!

On July 14 we issued a press release about an FBI cybersnooping device code-named Carnivore, which can scan millions of e-mails per second. Because Carnivore has unlimited power to spy on almost everyone with an e-mail account, it may be the biggest threat to your digital
privacy ever.

Almost immediately after the existence of this project was disclosed in a July 11 Wall Street Journal article, public outrage began to mount -- and now Congress has been pressured into holding hearings on Carnivore.

To capitalize on Monday's hearing before a House Judiciary Committee panel, we've launched a campaign to "Kill the Carnivore"!

Politicians on Capitol Hill may be planning to mollify the public by starting an "investigation" into the system, but that's not enough: We want to stop the Carnivore in its tracks and kill it -- before it devours your privacy.

Please read this e-mail and "IMMEDIATELY" take the action below. Then forward this e-mail to friends, and ask them to do the same.

BACKGROUND:
Carnivore is a hardware-software device that the FBI secretly developed at its lab in Quantico, Va. Dubbed Carnivore because of its ability to find "the meat" among millions of e-mails, Carnivore scans every incoming and outgoing e-mail message on a network looking for telltale words or names, and saves those messages for later retrieval by

deja Career Center
• Job Search
• Post Resumes
• Career Tools
• For HR/Recruiters
and more!

Explore Now!

law enforcement. Carnivore can also track instant messages, visits to web sites, and Internet relay chat sessions.

The FBI admits that Carnivore will scan millions of e-mail messages from innocent people to find a tiny number of messages from people suspected of crimes. That's no different than if the FBI opened everyone's mail hoping to find a letter from a criminal, or listened in on everyone's phone calls just in case a crime was being discussed.

Though Carnivore's existence was just publicly revealed, the FBI has already installed the device at dozens of Internet Service Providers (ISPs) around the country, and claims it has used it "fewer than 50 times" so far. In many cases, the FBI keeps the device in a locked cage on the ISP's premises, with agents making daily visits to retrieve the captured data.

Many ISPs have refused to allow the FBI to install Carnivore, citing concerns that the privacy of all their customers could be violated. But earlier this year, a federal judge ruled against one such ISP, leaving it no choice but to allow the FBI access to its system.

Predictably, the FBI promises to limit surveillance to messages from suspected hackers, terrorists, or drug dealers. But considering that this is the same agency that quietly inserted "roving telephone tap" authority into federal law and illegally turned over confidential personnel files to the Clinton White House, you shouldn't be expected to trust it with your confidential e-mails.

But Carnivore is more than a threat to your ordinary e-mail correspondence -- it also gives government bureaucrats the ability to spy on your online banking transactions, because it has the ability to monitor all digital communications. The bottom line is that your privacy won't be protected as long as Carnivore is on the loose.

POST REPLY

<< previous in search · next in search>>

Subscribe to alt.comp.freeware
Mail this message to a friend
View original Usenet format
Create a custom link to this message from your own Web site

Search Discussions
For a more detailed search in Discussions go to Power Search
Search only in: alt.comp.freeware
All Deja.com
Search for: carnivore
Search
Search: repeat... discussions

Copyright © 1995-2000 Deja.com, Inc. All rights reserved.
Trademarks · Terms and Conditions of Use · Site Privacy Statement
Advertise With Us | About Deja.com | Careers @

Wolf Camera · Free Stuff@FreeShop · Tires.com · Deja e-centives · ELECTRONICS@SupremeVideo · TireRack.com · Cost+Pricing@eCOST
Search for Jobs! JobOptions · As Low as 2.9% Intro APR · Domain Registration · FREE SoftwareNEWcars@carOrder

weapon is slow, silent, invisible, and men perceive it only by its consequences - by the gutted ruins and the moans of agony it leaves in its wake. The name of the weapon is: inflation.
-- Ayn Rand, "Egalitarianism And Inflation," Philosophy: Who Needs It

ICQ: 9815080 [Disabled] Operator Taliesin_2 of #SacredNemeton on IRC PaganPaths

POST REPLY

<< previous in search · next in search>>

Subscribe to alt.comp.freeware
Mail this message to a friend
View original Usenet format
Create a custom link to this message from your own Web site

Search Discussions

Search

Copyright © 1995-2000 Deja.com, Inc. All rights reserved.
Trademarks · Terms and Conditions of Use · Site Privacy Statement

Advertise With Us | About Deja.com | Careers @

Wolf Camera · Free Stuff@FreeShop · Tires.com · Deja e-centives ELECTRONICS@SupremeVideo · TireRack.com · Cost+Pricing@eCOST · Search for Jobs! JobOptions · As Low as 2.9% Intro APR · Domain Registration · FREE SoftwareNEWcars@carOrder

Home
Custom Search
Dogpile Remote
Search at Home
Help with Syntax
MetaFind Search
Tell a Friend



DOGPILE
Web Metasearch Results

Lowest prices on the net for products and services
Home & Life • Collectibles • Travel • Small Business



Add ecommerce to your site	9-out-of-10 people prefer it to thumb-twiddling.	Ask any question you can think of - Free!

Buy books about "carnivore" at Amazon.com Search for "carnivore" on Electric Library

Are you looking for:			
Carnivorous Plants	Carnivores 2	Cherryhill Carnivorous	Carnivore Vietnam
Carnivores In Ecosystems	California Carnivores	Carnivores II	Carnivores Game

Search engine: Deja News found 30 documents.

The query string sent was carnivore

Date	Subject	Forum	Author
07/24/2000	Re: CNN Story on FBI Carnivo	comp.security.firewal	David
07/24/2000	Re: British law would allow	alt.comp.freeware	Taliesin2
07/24/2000	Carnivore	fido7.moldova.interne	Adrian Oboroc
07/23/2000	CNN Story on FBI Carnivore	comp.security.firewal	Andrew P. Hende
07/23/2000	Re: CNN Story on FBI Carnivo	comp.security.firewal	Andrew P. Hende
07/23/2000	Re: Carnivore is a Violation	talk.politics.misc	Maximum Acid
07/22/2000	Re: 'Carnivore' Won't Devour	alt.security.pgp	News
07/22/2000	CARNIVORE, THE ELECTRONIC GE	alt.conspiracy	roninart
07/22/2000	CARNIVORE THE ELECTRONIC GES	alt.politics.election	roninart
07/22/2000	Re: CARNIVORE, THE ELECTRONI	alt.conspiracy	Terry Jameson
07/22/2000	Re: 'Carnivore' Won't Devour	alt.privacy.spyware	husky
07/22/2000	FBI's Carnivore Page	alt.privacy	An Metet
07/22/2000	CARNIVORE THE ELECTRONIC GES	alt.politics	roninart
07/23/2000	Re: Does anyone know about t	alt.folklore.urban	Lara Hopkins
07/22/2000	Carnivore is a Violation of	talk.politics.misc	Secret Squirrel
07/22/2000	Re: Who'se ISPs are being mo	austin.internet	D. Cook
07/22/2000	announce@lp.org: Urgent Acti	alt.law-enforcement	Mark2101
07/22/2000	Lebedev le carnivore	fr.soc.economie	KAGANOVITCH
07/22/2000	Does anyone know about the C	alt.folklore.urban	William B. Swea
07/22/2000	Does anyone know about the C	alt.folklore.urban	William B. Swea
07/22/2000	Kill It!	alt.religion.w-w-chur	Janice Matchett
07/22/2000	Kill It!	alt.religion.w-w-chur	Janice Matchett
07/22/2000	Carnivore	talk.politics.guns	Silverdahl
07/22/2000	Carnivore	talk.politics.guns	Silverdahl
07/22/2000	Seems Clinton's and Reno's C	3dfx.products.voodoo5	Greg S. Trouw
07/22/2000	Re: announce@lp.org: Release	talk.politics.guns	rcain.nospam

07/22/2000	Re: announce@lp.org: Release	talk.politics.guns	rcain.nospam
07/22/2000	Re: Carnivore	talk.politics.guns	Cuchulain Libby
07/22/2000	Can carnivore be used to pre	alt.privacy	withheld
07/22/2000	Re: Can carnivore be used to	alt.privacy	Norm G.
07/22/2000	Re: Can carnivore be used to	alt.privacy	jungle

Search engine: AltaVista's Usenet Search found 100 documents.
The query string sent was +carnivore

Date	Subject	Forum	Author	
30 Jun	Nutritional Sources? Vegan, Vegetarian Vs Carnivore	yemenmocha@my-deja. com	alt.animals.ethics.veg...	
09 Jul	FA: OOP Carnivore and Rigor Mortis CDs	Michael Siciliano	alt.rock-n-roll.metal	
11 Jul	FBI's Carnivore	An Metet	alt.privacy.anon-server	
11 Jul	More on FBI's Carnivore	An Metet	alt.privacy	
11 Jul	More Info On Carnivore, The Wire the FBI Have On Your ISP	OsioniusX	alt.fan.cult-dead-cow	
11 Jul	Carnivore	Glen Harman	news.admin.net-abuse.e...	
11 Jul	URGENT--- FBI's Carnivore may be on your ISP!	Lazyike	rec.drugs.misc	
	Carnivore Eats Your Privacy	11 Jul		3 Discordia SCC (alt.discordia.scc)
11 Jul	RE:CARNIVORE	Anonymous	alt.privacy	
11 Jul	Big Brother's carnivore program*-*-	Fred	alt.privacy.anon-server	
11 Jul	OT - Superfast system called 'Carnivore' searches e-mails for messages	Ronald Gillen	soc.culture.baltics	
11 Jul	FBI's CARNIVORE system	Jose Vellancemp, Esquire	alt.drugs.pot	
11 Jul	Interesting Editorial on Carnivore	the Pull	alt.fan.cult-dead-cow	
11 Jul	Carnivore Letter Printed in Entirety	the Pull	alt.fan.cult-dead-cow	
11 Jul	Carnivore in nyc.transit means no.privacy!	No User	nyc.transit	
12 Jul	The Emeraude Project, French Carnivore+Echelon	nobody@nowhere.com	alt.privacy.anon-server	
11 Jul	Carnivore: Who Cares ... zzzzzzzz	Dan	alt.privacy.anon-server	
12 Jul	ACLU: Law Needs 'Carnivore' Fix	Viviane Lerner	flora.mai-not	

	'Carnivore' Fix		
12 Jul	Carnivore Causing concern	Jeremy Compton	bit.listserv.cloaks-da...
12 Jul	FBI Big Brother Carnivore + Privacy Resources	E Right	alt.politics.bush

There is 1 search engine left to be searched. For more results, click below.

Next Set of Search Engines

Are you looking for:			
Carnivorous Plants	Carnivores 2	Cherryhill Carnivorous	Carnivore Vietnam
Carnivores In Ecosystems	California Carnivores	Carnivores II	Carnivores Game

Buy books about "carnivore" at Amazon.com Search for "carnivore" on Electric Library



DOGPILE SEARCH GEOGRAPHIC SEARCH

carnivore Fetch

○ Web Metasearch ○ Web Catalog ◉ Usenet ○ Newscrawler ○ BizNews ○ Ftp

○ Stock Quotes ○ Jobs/Careers ○ Weather ○ Auctions ○ Images NEW

○ Yellow Pages ○ White Pages ○ Maps ○ Audio/MP3

Texis & Webinator Copyright (C) 1997 THUNDERSTONE - EPI, Inc.

Telecoms Miffed at FBI Meddling

by Declan McCullagh

3:00 a.m. Jul. 8, 2000 PDT

A telecommunications trade association this week criticized a recent FBI move to thwart the $5.5 billion sale of ISP Verio to a Japanese firm.

The FBI's objections that the Fed agency may not be able to conduct the kind of Internet surveillance it desires are specious, said the Computer and Communications Industry Association.

Everybody's got issues in Politics
More Funding for FBI Snooping

"In taking this action the FBI runs the serious risk of frustrating the openness of Internet communications, infringing our civil liberties, and damaging our relations with important trading partners," said Ed Black, president of the CCIA. The groups' members include AT&T, Nortel, Nokia, and NTT America, the Japanese company which hopes to purchase Verio.

Last year, the FBI unsuccessfully asked the Internet Engineering Task Force to build wiretap capabilities into protocols. FBI Director Louis Freeh has, in the past, asked Congress for domestic controls on data-scrambling encryption products and successfully pressed for a "digital telephony" law that requires telephone companies to ensure that their networks are able to be tapped by the Feds.

Anti-anonymity: If you criticize a Pennsylvania judge online, be warned: You may not be as anonymous as you thought.

Thin-skinned Superior Court Judge Joan Orie Melvin in early 1999 sued over a dozen "John Does" that she suspected of posting messages on a muckraking site devoted to Pittsburgh politics.

A judge who recently heard arguments in Melvin's case will decide whether or not to unmask the folks who participated in the "Grant Street 99" site, according to an article in the *Pittsburgh Tribune-Review*,.

The ACLU is defending the John Does, including one who reportedly alleged that Judge Melvin was engaged in surreptitious and -- if true -- unlawful partisan political activity.

Bill Joy a Killjoy? An article on the website of the conservative *National Review* takes aim at Bill Joy of Sun Microsystems, who recently raised eyebrows when he warned of the dangers of unregulated technology.

Authors Glenn Reynolds and Dave Kopel said Joy's article, published earlier this year in *Wired Magazine*, is an example of "neo-Luddite sentiment."

"More generally, Luddite intellectuals are successfully propagating 'the precautionary principle,' which states that we should never try anything new unless we are certain that it is absolutely safe... Even worse, "relinquishment" would probably accelerate the progress of destructive nanotechnology. In a world where nanotechnology is outlawed, outlaws would have an additional incentive to develop nanotechnology," the National Review authors wrote.

Upcoming events: Two U.S. senators are holding a briefing on medical and genetic privacy on

Doc. #19

July 14. The event, sponsored by the Forum on Technology Innovation is scheduled for 12:15 p.m. in room 325 of the Russell Senate office building... The Freedom Forum is releasing its state of the First Amendment survey on July 13 at 9 am... A federal online "child protection" commission meets July 20 in Richmond.

Related Wired Links:

ICANN Gets Mixed Review
Jul. 7, 2000

Oracle's Hot Summertime Fund
Jul. 1, 2000

Feds' Hands Caught in Cookie Jar
Jun. 30, 2000

How Congressional Cookies Crumble
Jun. 30, 2000

McCain Renews Porn-Filter Push
Jun. 28, 2000

'Twas Oracle That Spied on MS
Jun. 28, 2000

DOJ's Got the Antitrust Itch
Jun. 28, 2000

Copyright © 1994-2000 Wired Digital Inc. All rights reserved.

FBI taps of e-mail provoke concerns

Privacy issues lead to House hearings on 'Carnivore' work; Name called 'unfortunate'

By Del Quentin Wilber
Sun National Staff

WASHINGTON -- To civil libertarians and Internet service providers, a device created by the FBI to snoop through e-mail messages is as ominous as its name: "Carnivore."

Attached to an ISP's server, the contraption sifts through countless e-mail messages and copies specific information for federal agents seeking suspected criminals, including terrorists and child pornographers.

But critics say that, in the process of sifting out communications from its targets, Carnivore is also capable of retrieving the private messages of innocent people.

"This is a very dangerous device," said Barry Steinhardt, associate director of the American Civil Liberties Union. "It's unprecedented. It's the first time law enforcement has carte blanche access to the entire service provider's network."

The controversy surrounding the device with the foreboding name has caught the attention of Republican lawmakers, and a House Judiciary subcommittee is scheduled to hold a hearing on the matter today. Opponents and authorities who support the use of Carnivore are scheduled to testify.

After the system was disclosed in recent news accounts, sparking criticism from privacy advocates, FBI officials met with lawmakers and reporters to try to show that Carnivore is not nearly as intrusive as some fear.

For one thing, FBI officials said, they need the device to combat crime and threats to national security. They describe Carnivore as a "surgical" tool that would protect ordinary people from unintended searches.

"There are filtering mechanisms built in that limit the amount of information viewable to the human eye," said Paul Bresson, a spokesman for the bureau. "It ensures that only the exact communications authorized by a court are what we intercept."

For decades, federal agents and local police have been wiretapping suspects' phones after obtaining permission from judges. But those wiretaps are limited to a specific suspect and do not comb through phone calls at random.

Carnivore works much differently, though authorities still must obtain permission from a judge to scour e-mail messages or discover which Web pages a suspect visits.

Once they have court approval, agents attach the Carnivore device -- an

DOC. #20

ordinary-looking desktop computer -- to the ISP's main computer, and Carnivore "passively" sniffs through streams of data, FBI officials said.

Carnivore does not read e-mail messages or their subject lines, officials said. Instead, it searches for computer codes that direct the message to and from the suspect. Nor can it scan e-mail messages for key words, like "drugs or bomb," an FBI official said.

In other words, authorities say, Carnivore acts like an FBI agent authorized to scan envelopes sent by mail. The agent seeks a particular suspect's addressing information and pulls aside any qualified envelope and opens it.

Last week, after an outcry from critics, the White House said it would propose legislation to, among other things, require agents to seek Justice Department clearance before asking judges to authorize the use of Carnivore in a specific case. Such rules already cover voice wiretaps.

But the proposal was dismissed by civil liberties groups, who said it did not go far enough in protecting electronic communication.

For their part, FBI officials say, the White House proposal is not necessary: They say they abide by the rules governing voice wiretaps to use Carnivore.

Despite the assurances of FBI officials, civil liberties groups and congressional Republicans say they are wary of the system.

"It has the capability of grabbing it all," said Richard Diamond, a spokesman for Rep. Dick Armey, the Texas Republican who is the House majority leader and a sharp critic of Carnivore. "It all depends on who pushes the button. Someone could push the wrong button and have access to all sorts of information."

FBI officials dispute that assertion, though they concede that Carnivore has sometimes captured e-mail messages and data that were not targeted in their searches. They say they sealed such information and did not read it.

Earlier this year, an ISP tried unsuccessfully to prevent FBI agents from installing Carnivore on its network. After a brief court fight, the company, Earthlink, yielded to FBI demands and helped install the device.

FBI officials say they don't mind simply asking ISPs to provide them with e-mail sent by criminal suspects if that is possible. But, in most cases, agents would rather use Carnivore because it helps maintain security for criminal evidence. And many smaller ISPs are not capable of creating programs to obtain the necessary data, FBI officials said.

Though most ISPs have complied with court orders to install Carnivore, one major provider said it would refuse.

"We're not going to stand for this," said William L. Schrader, chairman and chief executive officer of PSINet Inc. "It's insidious. If they were to ask us with a court order to violate the privacy of all our customers, we would take this to the Supreme Court."

Authorities say that more criminals, especially those involved in child pornography and fraud, are increasingly using the Internet and e-mail to commit crimes.

About three years ago, agents and federal prosecutors began asking for real-time access to e-mail and Web-site visits, FBI officials said. The agents said they were worried about not having reliable and up-to-date intelligence.

FBI technicians began developing Carnivore, which was used for the first time about 18 months ago, authorities said. FBI officials declined to disclose any information about Carnivore-related cases but said the system has been used fewer than 25 times.

FBI officials said the "unfortunate" choice of a name emerged during internal discussions of the program. At first, technicians called it "Omnivore" because it ate everything in sight. But as the system became more refined, technicians felt it needed a better name and changed it to Carnivore: a meat-eater.

"We're looking at how we name a lot of projects right now," an FBI official said. "This has been sobering."

FBI agents noted that they don't need Carnivore to read most old e-mail messages stored on ISP servers; they can already do so with court approval.

They described the Carnivore system as a last-resort measure to capture real-time communications.

Authorities on technology and society say they are hardly surprised that the system has generated anxiety, because many people now send more personal information over e-mail than over the phone.

Corporate snooping of employee e-mail and the unauthorized sale of client information by e-retailers have unnerved many computer users.

Originally published Jul 24 2000



CLICK HERE!



USA TODAY Tech Report

provided by Bloomberg

Fulton Street
FREE Same Day Delivery

Service Magic
Quality Contractors for 485 services.

Hollywood.com
Free gift with $25.00 purchase.

07/21/00- Updated 04:19 PM ET

Send this story to a friend

FBI: 'Carnivore' will play nice

During demonstration, details of e-mail 'wiretap' system emerge

WASHINGTON (Bloomberg) — The FBI's Carnivore e-mail surveillance system won't snoop on innocent Internet users, officials said Friday.

FBI officials gave reporters a demonstration of the system they say adopts traditional telephone wiretap methods to the Internet without violating the rights of law-abiding Web surfers.

From our archive:

- Clinton proposes updated wiretap laws
- FBI e-mail snooping sparks controversy
- Reno reviewing FBI's Net 'wiretap' system

The disclosure that the FBI and Internet service providers have cooperated to bug the messages of criminal suspects has generated criticism from civil liberties groups and some Republican lawmakers. They say Carnivore will let the FBI see e-mails of all Internet subscribers, not just the few suspects the FBI wants to track.

FBI officials will defend Carnivore Monday before a U.S. House Judiciary subcommittee headed by Republican Henry Hyde of Illinois.

Earlier this week, the Clinton administration proposed limiting law enforcement wiretapping of e-mail to investigations of serious crimes and requiring top-level Justice Department authorization of e-mail

Search
the site the Web
go
POWERED BY LYCOS

Inside Tech
Talk Tech
FAQ/Tips
Web Column
Hot Sites
Tech News
Tech Investor
Tech Reviews
Answer Desk
Game Zone

Doc. #21

Daily Digest
Shareware Shelf
Web Potholes
Web Resources
Consumer Sites
Tech Front

Marketplace
Hardware
Accessories
Software

Print Edition
Today
Yesterday
Subscribe
Archive

Find books up to 50% off!
BARNES&NOBLE

Resources
E-mail
Site map
Feedback
About us
Jobs at USA TODAY

Free premiums
USA TODAY Update
Software

USA TODAY .com Users!

bugging. Under proposed legislation, the procedures for e-mail surveillance would be similar to those in place for telephone surveillance.

Court order

Electronic tapping of an Internet service provider's data traffic requires a court order. No judge has rejected the government's application for a court order to connect Carnivore to the computer servers of private Internet companies.

These servers contain mountains of data traffic generated by millions of subscribers. Internet companies generally let FBI officials who come to their offices monitor the companies' Internet messages, FBI officials said.

The FBI said it's looking for two academic institutions to serve as outside auditors to ensure the FBI doesn't overreach its authority and pry into the online communications of the general public.

FBI officials said Carnivore has been used 25 times in the past year. It was introduced three years ago.

Carnivore uses a "filter," which is a computer containing proprietary software the FBI buys from private companies. The filter will connect to the servers of Internet companies to weed out messages sent and received by people unconnected to the investigation, officials said, speaking on condition of anonymity. They said the Carnivore filter blocks law-enforcement officials from seeing the e-mail of innocent bystanders.

Big Internet companies already have their own filtering systems that screen messages to be seen by the FBI and spare agents from reviewing extraneous data, officials said.

SAVE TIME! CHECK OUR REAL-TIME FLIGHT TRACKER USA TODAY .com

Front page, News, Sports, Money, Life, Weather, Marketplace

© Copyright 2000 USA TODAY, a division of Gannett Co. Inc.

GOP.gov

HOUSE REPUBLICAN CONFERENCE

J.C. WATTS, JR.
CHAIRMAN
4th District, Oklahoma

Reforming Washington
Securing America's Future

News Release

For Immediate Release
Monday, July 24, 2000

Contact: Ron Bonjean/Kevin Schweers
(202) 225-5107

Watts: FBI's 'Carnivore' System a Dangerous Invasion of Privacy

Calls on Clinton-Gore Administration to Suspend New Surveillance Program

WASHINGTON – Rep. J.C. Watts, Jr. (R-OK), Chairman of the House Republican Conference and House Republican Cyber-Security Team, issued the following statement today on the FBI's "Carnivore" system at a Capitol Hill hearing:

"We need innovative, new law enforcement strategies to combat the real and growing threat of cyber-crime. U.S. law enforcement needs to focus resources on the training and expertise necessary to protect our cyber-security. I remain committed to working in Congress to adequately invest in and support the right law enforcement tactics.

"However, the FBI's 'Carnivore' program represents a dangerous and unprecedented invasion of online privacy. Despite repeated inquiries, the Clinton-Gore Administration continues to offer only vague responses and little enlightenment.

"The FBI's record on protecting privacy is also problematic. From unwarranted wiretaps to its mishandling of hundreds of files on political appointees just a few years ago, there is ample cause for concern.

"Before we impose privacy restrictions on the commercial industry, it seems the federal government has a duty and an obligation to honor the privacy of the people it has sworn to protect. I commend Chairman Canady for highlighting this egregious threat to the online privacy of every American."

-- END --

C-SPAN.ORG PUBLIC AFFAIRS ON THE WEB
CREATED BY AMERICA'S CABLE COMPANIES
SITE INDEX
TV Schedule | Classroom | LIVE TV/Radio | Community | About C-SPAN | Shop C-SPAN

House Committee

FBI E-Mail Surveillance Program

Judiciary
Washington, District of Columbia (United States)
Rayburn House Office Building,
ID: 158376 - 07/24/2000 - 2:00 - No Sale

Hyde, Henry J., U.S. Representative, R-IL
Baker, Stewart, Attorney
Corn-Revere, Robert, Attorney
DiGregory, Kevin, Deputy Assistant Attorney Gene, Department of Justice
Steinhardt, Barry, Associate Director, American Civil Liberties Union
Kerr, Donald, Director, Federal Bureau of Investigation, Crime Lab

Committee members hear testimony on a computer program called 'Carnivore' that will allow the FBI to intercept and collect electronic communications that are the subject of court orders.

For more information please contact viewer@c-span.org.

Copyright © 2000 National Cable Satellite Corporation

Doc. #23

C-SPAN Networks
Schedule for Monday, 07/24/2000

All Times E.D.T.
Fri Sat Sun Mon Tue Wed Thu

Previous Day 07 / 24 / 2000 Go! Next Day

Current 3 Months
Search the C-SPAN Schedule

Back to Current Schedule

C-SPAN

Time	Program
07:00 am 1:15 (est.) *LIVE*	Call-In Open Phones C-SPAN, Washington Journal
08:15 am 0:45 (est.) *LIVE*	Call-In Diplomatic Meetings C-SPAN, Washington Journal Massimo Calabresi , *TIME* Magazine
09:00 am 0:30 (est.) *LIVE*	Call-In The History of Philadelphia C-SPAN, Washington Journal
09:30 am 0:30 (est.) *LIVE*	Call-In Benjamin Franklin C-SPAN, Washington Journal
10:03 am 1:14 (est.)	Call-In Open Phones C-SPAN, Washington Journal
11:20 am 0:43 (est.)	Call-In Diplomatic Meetings C-SPAN, Washington Journal Massimo Calabresi , *TIME* Magazine
12:06 pm 0:03 (est.)	Call-In The History of Philadelphia C-SPAN, Washington Journal

C-SPAN 2

Time	Program
08:01 am 1:25 (est.)	Speech Nurse Shortage Forum on Health Care Leadership Leah Curtin , *Curtin Calls*
09:26 am 0:22	TBA
09:49 am 0:26 (est.)	Speech Expanding the Republican Congressional Majority Virginia Young Republicans Tom Davis , R-VA
10:22 am 0:56 (est.)	National Press Club Speech Technology and Global Democratization National Press Club Robert Davis , Lycos, Inc.
11:21 am 0:36 (est.)	News Conference Republican Delegates Platform Poll American Conservative Union Donald Devine , Forbes Presidential Campaign
12:00 pm 7:00 (est.) *LIVE*	Senate Proceeding Senate Session U.S. Senate *The beginning and end of this live program may be earlier or later than the scheduled times.*

12:09 pm 0:20 - TBA -

12:30 pm House Proceeding
0:30 Morning Hour
(est.) U.S. House of Representatives
LIVE *The beginning and end of this live program may be earlier or later than the scheduled times.*

01:00 pm 0:48 - TBA -

01:48 pm Call-In
0:28 Benjamin Franklin
(est.) C-SPAN, Washington Journal

02:00 pm House Proceeding
1:45 House Session
(est.) U.S. House of Representatives
LIVE *The beginning and end of this live program may be earlier or later than the scheduled times.*

03:45 pm News Conference
0:39 Protests at the Republican Convention
(est.) R2D2 Coalition

04:24 pm 1:35 - TBA -

06:00 pm House Proceeding
3:00 House Session
(est.) U.S. House of Representatives
LIVE

Programs Airing Monday, 07/24/2000, not yet Scheduled

Length	Network	Program
0:00	- TBA -	Archbishop Tutu Farewell
0:00	- TBA -	Georgia Senator Appointment
8:31	- TBA -	Treasury Issues

C-SPAN Extra

Time	Program
07:00 am 6:00	TBA
01:00 pm 2:00 (est.) *LIVE*	House Committee FBI E-Mail Surveillance Program Judiciary Henry J. Hyde , R-IL Stewart Baker *The beginning and end of this live program may be earlier or later than the scheduled times.*
03:00 pm 1:00	TBA
04:00 pm 1:00 (est.) *LIVE*	House Committee Presidential Requirement Amendment Judiciary, Constitution Forrest McDonald , University of Alabama Charles Canady , R-FL *The beginning and end of this live program may be earlier or later than the scheduled times.*

C-SPAN Radio

Time	Program
07:00 am 6:00	TBA
01:00 pm 2:00 (est.) *LIVE*	House Committee FBI E-Mail Surveillance Program Judiciary Henry J. Hyde , R-IL Stewart Baker *The beginning and end of this live program may be earlier or later than the scheduled times.*
03:00 pm 1:00	TBA
04:00 pm 1:00 (est.) *LIVE*	House Committee Presidential Requirement Amendment Judiciary, Constitution Forrest McDonald , University of Alabama Charles Canady , R-FL *The beginning and end of this live program may be earlier or later than the scheduled times.*

For more information please contact schedule@c-spanarchives.org.

Copyright © 2000 National Cable Satellite Corporation

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF GENERAL COUNSEL
INVESTIGATIVE LAW UNIT
(THROUGH 7/28/00)

PAGES REVIEWED: 132

PAGES RELEASED: 132

EXEMPTIONS CITED: b6-1, b7C-1, b6-3 & b7C-3

NOTE: 29 Pages from this file are duplicates to pages from The Office of General Counsel's Front Office file and The Office of General Counsel/Technology Law Unit's file.

[redacted]

b6-1/b7c-1

Department Of Justice
Office Legislative Affairs
Control Sheet

Date Of Document: 02/29/00
Date Received: 02/29/00
Due Date: 03/08/00

Control No.: 000301-346
ID No.: 364179

From: OMB (S.2092) (LRM-REJ280) ((106TH CONGRESS))
To: OLA

Subject:
REQUEST FOR VIEWS ON S.2092, HIGH TECH CRIME BILL

Action/Information: Signature Level: OLA

Referred To:	Date Assigned:	Action:
CRM, FBI, DAG, OLC, OPD	03/01/00	FOR YOUR INFORMATION - PREVIOUSLY CIRCULATED UNDER CONTROL NO 000228 315. CC: OLA [redacted] b6-3/b7c-3

Remarks:

Comments:

File Comments:
Primary Contact: [redacted] b6-3/b7c-3

Translate for R&C

DOC #1

WED 15:05 FAX 202 5[illegible]3485 DOJ OLA [illegible] FAX
2000 20:52 TO:61 - JUSTICE FROM: [redacted] P. 1/8

b6-3
b7C-3

Total Pages: 8

LRM ID: REJ280

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
Washington, D.C. 20503-0001

Tuesday, February 29, 2000

LEGISLATIVE REFERRAL MEMORANDUM

b6-3
b7C-3

TO: Legislative Liaison Officer - See Distribution below

FROM: Richard E. Green (for) Assistant Director for Legislative Reference
OMB CONTACT: [redacted]
E-Mail: [redacted]omb.eop.gov
PHONE: (202[redacted] FAX: (202[redacted]

SUBJECT: OMB Request for Views on S2092 High Tech Crime Bill

DEADLINE: Wednesday, March 8, 2000

In accordance with OMB Circular A-19, OMB requests the views of your agency on the above subject before advising on its relationship to the program of the President. Please advise us if this item will affect direct spending or receipts for purposes of the "Pay-As-You-Go" provisions of Title XIII of the Omnibus Budget Reconciliation Act of 1990.

COMMENTS: A copy of S. 2092 is attached.

Justice: Please advise of any plans to prepare a views letter on S. 2092.

DISTRIBUTION LIST

AGENCIES:
61-JUSTICE - Robert Raben - (202) 514-2141
114-STATE - Paul Rademacher - (202) 647-4463
29-DEFENSE - Samuel T. Brick Jr. - (703) 697-1305
118-TREASURY - Richard S. Carro - (202) 622-0650
25-COMMERCE - Michael A. Levitt - (202) 482-3151
36-Federal Communications Commission - Sheryl Wilkerson - (202) 418-1900
21-Central Intelligence Agency - Cynthia D. Erskine - (703) 482-8626

EOP:
Barbara M. Fahy
Leanne A. Shimabukuro
Deanne E. Benos
Peter P. Swire
Lauren B. Steinfeld
Martin L. Young
Glenn R. Schlarman
Thomas A. Kalil
David W. Beier
James M. Kulikowski

b6-3
b7C-3

[illegible]d H. Chase
[illegible]y Jo Sicari
Joanne Chow
Anne R. Stauffer
Charles W. Fox
Ellen J. Balis
Pamula L. Simms
Nell Lobron

tion 6412(a)(1) of such Code is ... by inserting "(the date of the enactment of the American Transportation Recovery Act of 2000, in the case of diesel fuel)" after "October 1, 2005" both places it appears.

(B) by inserting "(the date which is 6 months after the date of the enactment of such Act, in the case of diesel fuel) after "March 31, 2006" both places it appears, and

(C) by inserting "(the date which is 3 months after the date of the enactment of such Act, in the case of diesel fuel) after "January 1, 2006".

(4) Section 6427(l)(4) of such Code is amended by inserting "(during the 1 year period beginning on the date of the enactment of the American Transportation Recovery Act of 2000, in the case of diesel fuel)" after "September 30, 2007".

(c) EFFECTIVE DATE.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendments made by this section shall take effect on the date of the enactment of this section.

(2) DECREASE IN CRUDE OIL PRICES.—If the Secretary of Treasury determines that the average refiner acquisition costs for crude oil are equal to or less than such costs were on December 31, 1999, the amendments made by this section shall cease to take effect and the Internal Revenue Code shall be administered as if such amendments did not take effect.

By Mrs. FEINSTEIN:

S. 2091. A bill to amend the Act that authorized construction of the San Luis Unit of the Central Valley Project, California, to facilitate water transfers in the Central Valley Project; to the Committee on Energy and Natural Resources.

THE CONSTRUCTION OF THE SAN LUIS UNIT OF THE CENTRAL VALLEY PROJECTS

Mrs. FEINSTEIN. Mr. President, today I introduce a bill to amend the legislation that authorized construction of the San Luis Unit of the Central Valley Project in California. Enactment of this bill would allow water districts in the San Luis Unit of the Central Valley Project to supplement their federal water supplies with purchases of water from the State Water Project. At present, federal law prohibits the delivery of non-federal water to districts in the San Luis Unit until certain conditions are met.

The San Luis Unit is the last component created by federal law in the Central Valley Project, which is the largest Bureau of Reclamation project in the United States. Water service to districts in the San Luis Unit is often curtailed because of limitations imposed in pumping in the Sacramento-San Joaquin Delta.

It is customary for water districts in the San Luis Unit to supplement their supplies through purchases on the open market. However, current federal law prohibits them from purchasing supplies from the State Water Project and having these delivered over federal facilities. Making such deliveries is relatively easy because state and federal project conveyance facilities are interconnected. Prohibiting purchase of state water for delivery over federal facilities limits the opportunities available for San Luis Unit districts to obtain as large a supplemental supply as they would like.

Mr. President, this bill has already passed the House as H.R. 3077. It will impose no additional costs on the federal government. It contains provisions which assure that the additional water obtained by districts in the San Luis Unit cannot be used in a manner that would exacerbate current groundwater drainage problems. It is consistent with the provisions in the Central Valley Project Improvement Act that sought to encourage the exchange of water by willing sellers to provide additional supplies at reasonable cost to willing buyers. I urge the Senate to pass this bill.

By Mr. SCHUMER (for himself and Mr. KYL):

S. 2092. A bill to amend title 18, United States Code, to modify authorities relating to the use of pen registers and trap and trace devices, to modify provisions relating to fraud and related activities in connection with computers, and for other purposes; to the Committee on the Judiciary.

HIGH TECH CRIME BILL

Mr. SCHUMER. Mr. President, I rise today to introduce with my friend from Arizona, Senator KYL, a high tech crime bill aimed at combating computer crime. For the past nine months I have been discussing with law enforcement and computer crime experts how best to address the growing threat that computer crimes pose to our increasingly networked society.

Many of the best solutions are far-reaching and complex and will only be achieved through sustained and thoughtful hard work on an international level by both government and the private sector in the years ahead. There are, however, modes changes to existing laws that can be made now, which will serve as a significant first step in a much-needed effort to give law enforcement to tools they need to effectively fight cybercrime. The legislation that Senator KYL and I are introducing today will, among other things, make the following changes to existing law.

We must update our laws governing the use of what are called pen registers (which record the numbers dialed on a phone line) and trap and trace devices (which capture incoming electronic impulses that identify the originating number). These laws have become outdated and their procedures are too slow for the speed of criminals online.

Under current law, investigators must obtain a trap and trace order in each jurisdiction through which an electronic communication is made. Thus, for example, to trace on online communication between two terrorists that starts at a computer in New York, goes through a server in New Jersey, bounces off a computer in Wisconsin, and then ends in San Francisco, investigators may be forced to go successively to a court in each jurisdiction for an order permitting the trace (not to mention having to approach each provider along the way). In the recent Denial of Service attacks, hackers utilized dozens or even hundreds of "zombie" computers from which the attacks on specific sites were then launched. No doubt, these computers were located all over the country, and tracing them quickly under current law is therefore virtually impossible.

This legislation will amend current law to authorize the issuance of a single order to completely trace an online communication to its source, regardless of how many intermediate sites it passes through. Law enforcement must still meet the exact same burden to obtain such an order; the only difference is that they will not have to repeat this process over and over each time a communication passes to a new carrier in a different Jurisdiction.

One deficiency of the Computer Fraud and Abuse Act, 18 U.C.C. §1030, is its requirement of proof of damages in excess of $5,000. In several cases, prosecutors have found that while computer intruders had attempted to harm computers vital to our critical infrastructures, such as telecommunications and financial services, damages of $5,000 could not be proven. Nevertheless, these intrusions pose a great risk of harm to our country and must be prosecuted, punished, and deterred.

The Schumer-Kyl bill will unambiguously permit federal jurisdiction at the outset of an unauthorized intrusion into critical infrastructure systems rather than having investigators wait for any damage assessment. Crimes that exceed the $5,000 limit will be prosecuted as felonies, while crimes below that amount will be defined as misdemeanors. The bill will also clarify that a $5,000 loss resulting from a computer attack may include the costs of responding to the offense, conducting a damage assessment, restoring a system to its original condition, and any lost revenue or costs incurred as a result of an interruption in service. The $5,000 requirement should not serve as a barrier to the prosecution of serious computer criminals who threaten our country's networks.

This legislation will also modify a directive to the sentencing commission contained in the Anciterrorism and Effective Death Penalty Act of 1996, which required a mandatory minimum sentence of six months' imprisonment for certain violations of section 1030. Computer intrusions that violate the statute vary in their severity and maliciousness. All violations should be punished, but under the current regime the mandatory imprisonment applies to some misdemeanor charges, even where the attack caused no damage. As a result, some prosecutors have declined to bring cases, knowing that the result would be mandatory imprisonment. We should insure that federal prosecutors are bringing cases under section 1030, but we also should insure that the sentences being meted out fit the crime.

most technologically savvy are juveniles who have up with computers always at ir fingertips. Unfortunately, certain juveniles are committing the most serious computer crimes and wreaking havoc on our critical infrastructures. For example, one juvenile hacker caused an airport in Worcester, Massachusetts to shut down for over six hours when its telecommunications connections were brought down. Similarly, two California teenagers broke into sensitive military computers, including those at Lawrence Livermore National Laboratory and the U.S. Air Force.

As a longer term strategy, we need to do a better job of teaching our children from a very young age that, like anywhere else, certain conduct on the Internet is wrong and illegal. But we also need to send a clear message that crimes on the Internet will have real consequences. This legislation will amend 18 U.S.C. §1030 to give federal law enforcement authorities the power to investigate and prosecute juvenile offenders of computer crimes in appropriate cases. The bill will make juveniles fifteen years of age or older who commit the most serious violations of section 1030 eligible for federal prosecution in cases where the Attorney General certifies that such prosecution is appropriate. In conjunction with the elimination of the six-month mandatory minimum, this legislation will provide a balanced, measured approach to juvenile hacking crimes.

Again, these are just the first steps that should be taken in a very long battle against cybercrime that many of us will wage for years to come. And while we fight computer crime by modifying our criminal laws, we also should seek concomitant ways to fully protect the fundamental rights of innocent individuals on the Internet.

I want to thank Senator KYL for joining me in introducing this bill. As chairman of the Subcommittee on Technology, Terrorism, and Government Information, I know that he cares deeply about these issues and I look forward to working with him on this commonsense, bipartisan legislation.•

By Mr. DOMENICI (for himself, Mr. BINGAMAN, and Mr. BAUCUS):

S. 2893. A bill to amend the Transportation Equity Act for the 21st Century to ensure that full obligation authority is provided for the Indian reservation roads program; to the Committee on Environment and Public Works.

THE TRANSPORTATION EQUITY ACT FOR THE 21ST CENTURY AND INDIAN RESERVATION ROADS

• Mr. DOMENICI. Mr. President, I am pleased today to be joined by my colleagues JEFF BINGAMAN and MAX BAUCUS in introducing legislation to preserve precious dollars allocated by the Congress and the President for construction of Indian reservation roads.

There is no doubt that the Indian reservation road system is the poorest in our nation, and every federal dollar allocated for improving this situation should be directed to our nation's Indian reservations. The lack of adequate roads and bridges is a chronic problem on Indian reservations, where unemployment averages 35 percent and more than half of American Indian live in hard poverty.

Since 1982, when my Senate amendment added Indian roads to our federal highway trust fund accounts, all funds allocated for Indian roads have been used for that purpose. In ISTEA, which preceeded the enactment of the Transportation Efficiency Act for the 21st Century (TEA-21), the Indian Reservation Roads (IRR) program reached a level of $191 million per year.

Many of us in Congress worked hard to increase this IRR funding to $225 million in the first year of TEA-21 (FY 1998), and $275 million each year thereafter, through FY 2003. Unfortunately, a little noticed provision for Federal Lands Highways, placing an "obligation limitation" on the IRR program, has resulted in the transfer of funds intended for Indian reservations to be transferred to the 50 states.

In FY 1998, the amount deducted for this transfer to states from the IRR program was $24.2 million. In FY 1999, it was $31.7 million; and in FY 2000, the obligation limitation resulted in a loss of $34.9 million that could have been used for Indian reservation road building.

In all previous enacting legislation since 1982, federal funds intended for IRR programs have been used for IRR purposes. Only in TEA-21 was this changed due to the application of the obligation limitation to Federal Lands Highways and the IRR program.

Our bill will simply exclude the IRR program from this annual deduction that has totaled, in the past three years, more than $90 million. This money, while helpful to many states, is more badly needed on Indian reservations and should be preserved for that purpose. By excluding the IRR program from this obligation limitation provision, we will be increasing federal funds for Indian roads without increasing the cost of the total program. We will be focusing the funds for Indian roads on Indian roads, as we have intended since the IRR program first became part of our federal highway trust fund in 1982.

I urge my colleagues to join us in redirecting funds intended for Indian road construction to be dedicated to that purpose.•

Mr. BINGAMAN. Mr. President, I am pleased to join today with my good friend and colleague from New Mexico, Senator DOMENICI, to introduce this bill along with Senator BAUCUS. This bill assures that our Native American communities have the funding they need for critical transportation projects. Our bill will fund the Indian Reservation Road Program for the next three years with at least $275 million per year, the full amount authorized by Congress.

Mr. President, since I came to the Senate in 1983, I've worked hard to promote economic development and create new jobs for my state of New Mexico. One thing I learned very quickly is that you can't expect to attract new industry unless you have the basic infrastructure to support residential and commercial needs. The most important infrastructure needs include transportation, power, communications, water and sewers. Without these basic services at affordable rates, opportunities to create good jobs will simply not develop.

Today our country is fortunate to have one of the strongest economies in history. Our recent advances in job creation and economic growth are accomplishments that all Americans should be proud of. Unfortunately, as many of us know, some sectors of our nation continue to lag behind the wave of economic prosperity that has swept the nation. In particular, I remain concerned about our Native American communities. Unemployment rates today in Indian Country frequently top 30, 40, and even 50 percent. Mr. President, the nation must not stand by while Indian Country is literally being left behind. Perhaps more than any other community in America, the Tribes and Alaska Native Villages suffer from inadequate infrastructure.

This year I am pleased to be working with President Clinton, Senators DASCHLE, DOMENICI, and others on a number of new programs and initiatives to help the Native American Communities enjoy the same level of economic prosperity as the rest of America. In this respect, the Tribes are no different than the rest of America—to promote their economic development basic infrastructure must first be in place. The President's initiative recognizes this fact. The bill we are introducing today addresses one element of that initiative—the need for basic transportation, including roads and transit. This bill will help promote transportation on every reservation in America by fully funding the Indian Reservation Roads Program.

First established in 1928, the Indian Reservation Roads program is one of the ways America meets its special responsibility to help Native Americans achieve self sufficiency and self determination. The goal of the Indian Reservation Roads program is to provide safe and economic means of transportation throughout Indian Country. Over the years, the program has been reauthorized and modified to help meet the Tribes' needs for basic transportation infrastructure. Most recently, the program was reauthorized for six years in 1998. The program is playing a critical role in economic development, self-determination, and employment of Native Americans in 33 states, including the Alaska Native Villages.

Currently, the reservation roads system comprises 25,700 miles of BIA- and Tribal-owned roads and 25,600 miles of state, county and local roads. There

(1) by inserting "or trap and trace device" after "pen register";

(2) by inserting ", routing, addressing," after "dialing"; and

(3) by striking "call processing" and inserting "the processing and transmitting of wire and electronic communications".

(b) ISSUANCE OF ORDERS.—

(1) IN GENERAL.—Subsection (a) of section 3123 of that title is amended to read as follows:

"(a) IN GENERAL.—(1) Upon an application made under section 3122(a)(1) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order shall, upon service of the order, apply to any entity providing wire or electronic communication service in the United States whose assistance is required to effectuate the order.

"(2) Upon an application made under section 3122(a)(2) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court

O:\ARM\ARM00.115 S.L.C.

if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.".

(2) CONTENTS OF ORDER.—Subsection (b)(1) of that section is amended—

(A) in subparagraph (A)—

(i) by inserting "or other facility" after "telephone line"; and

(ii) by inserting before the semicolon at the end "or applied"; and

(B) by striking subparagraph (C) and inserting the following new subparagraph (C):

"(C) a description of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and".

(3) NONDISCLOSURE REQUIREMENTS.—Subsection (d)(2) of that section is amended—

(A) by inserting "or other facility" after "the line"; and

(B) by striking "or who has been ordered by the court" and inserting "or applied or who is obligated by the order".

(c) EMERGENCY INSTALLATION.—Section 3125(a)(1) of that title is amended—

(1) in subparagraph (A), by striking "or" at the end;

(2) in subparagraph (B), by striking the comma at the end and inserting a semicolon; and

(3) by inserting after subparagraph (B) the following new subparagraphs:

"(C) immediate threat to the national security interests of the United States;

"(D) immediate threat to public health or safety; or

"(E) an attack on the integrity or availability of a protected computer which attack would be an offense punishable under section 1030(c)(2)(C) of this title,".

(d) DEFINITIONS.—

(1) COURT OF COMPETENT JURISDICTION.—Paragraph (2) of section 3127 of that title is

amended by striking subparagraph (A) and inserting the following new subparagraph (A):

"(A) any district court of the United States (including a magistrate judge of such a court) or any United States Court of Appeals having jurisdiction over the offense being investigated; or".

(2) PEN REGISTER.—Paragraph (3) of that section is amended—

(A) by striking "electronic or other impulses" and all that follows through "is attached" and inserting "dialing, routing, addressing, or signalling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"; and

(B) by inserting "or process" after "device" each place it appears.

(3) TRAP AND TRACE DEVICE.—Paragraph (4) of that section is amended—

(A) by inserting "or process" after "a device"; and

(B) by striking "of an instrument" and all that follows through the end and inserting "or other dialing, routing, addressing, and signal-

ling information relevant to identifying the source of a wire or electronic communication;".

SEC. 2. MODIFICATION OF PROVISIONS RELATING TO FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

(a) PENALTIES.—Subsection (c) of section 1030 of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) in subparagraph (A)—

(i) by inserting "except as provided in subparagraphs (B) and (C)," before "a fine";

(ii) by striking "(a)(5)(C)," and inserting "(a)(5),"; and

(iii) by striking "and" at the end;

(B) in subparagraph (B)—

(i) by inserting "or an attempt to commit an offense punishable under this subparagraph," after "subsection (a)(2)," in the matter preceding clause (i); and

(ii) by adding "and" at the end; and

(C) by striking subparagraph (C) and inserting the following new subparagraph (C):

"(C) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an

offense under subsection (a)(5)(A) or (a)(5)(B), or an attempt to commit an offense punishable under this subparagraph, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

"(i) loss to one or more persons during any one-year period (including loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000 in value;

"(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

"(iii) physical injury to any person;

"(iv) a threat to public health or safety; or

"(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; and";

(2) by redesignating subparagraph (B) of paragraph (3) as paragraph (4);

(3) in paragraph (3)—

(A) by striking "(A)" at the beginning; and

O:\ARM\ARM00.115 S.L.C.

(B) by striking ", (a)(5)(A), (a)(5)(B),"; and

(4) in paragraph (4), as designated by paragraph (2) of this subsection, by striking "(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C)," and inserting "(a)(2), (a)(3), (a)(4), (a)(5),".

(b) DEFINITIONS.—Subsection (e) of that section is amended—

(1) in paragraph (2)(B), by inserting ", including a computer located outside the United States" before the semicolon;

(2) in paragraph (7), by striking "and" at the end;

(3) by striking paragraph (8) and inserting the following new paragraph (8):

"(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information;";

(4) in paragraph (9), by striking the period at the end and inserting "; and"; and

(5) by adding at the end the following new paragraphs:

"(10) the term 'conviction' shall include an adjudication of juvenile delinquency for a violation of this section; and

"(11) the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost or cost incurred because of interruption of service.".

(c) DAMAGES IN CIVIL ACTIONS.—Subsection (g) of that section is amended in the second sentence by striking "involving damage" and all that follows through the period and inserting "of subsection (a)(5) shall be limited to loss unless such action includes one of the elements set forth in clauses (ii) through (v) of subsection (c)(2)(C).".

(d) CRIMINAL FORFEITURE.—That section is further amended by adding at the end the following new subsection:

"(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

"(A) the interest of such person in any property, whether real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, whether real or personal, constituting or derived from any proceeds that such person obtained, whether directly or indirectly, as a result of such violation.

"(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any administrative or judicial proceeding relating thereto, shall be governed by the provisions of section 413 of the Controlled Substances Act (21 U.S.C. 853), except subsection (d) of that section.".

(e) CIVIL FORFEITURE.—That section, as amended by subsection (d) of this section, is further amended by adding at the end the following new subsection:

"(j)(1) The following shall be subject to forfeiture to the United States, and no property right shall exist in them:

"(A) Any property, whether real or personal, that is used or intended to be used to commit or to facilitate the commission of any violation of this section.

"(B) Any property, whether real or personal, that constitutes or is derived from proceeds traceable to any violation of this section.

O:\ARM\ARM00.115 S.L.C.

"(2) The provisions of chapter 46 of this title relating to civil forfeiture shall apply to any seizure or civil forfeiture under this subsection.".

SEC. 3. JUVENILE DELINQUENCY.

Clause (3) of the first paragraph of section 5032 of title 18, United States Code, is amended—

(1) by striking "or" before "section 1002(a)";

(2) by striking "or" before "section 924(b)"; and

(3) by inserting after ""or (h) of this title," the following: "or section 1030(a)(1), (a)(2)(B), or (a)(3) of this title, or is a felony violation of section 1030(a)(5) of this title where such violation of such section 1030(a)(5) is punishable under clauses (ii) through (v) of section 1030(c)(5)(C) of this title,".

SEC. 4. AMENDMENT TO SENTENCING GUIDELINES.

Section 805(c) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 28 U.S.C. 994 note) is amended by striking "paragraph (4) or (5)" and inserting "paragraph (5) or a felony violation of paragraph (5)(A)".

May 4, 2000

Mr. Parkinson:

Re: HIGH TECH CRIME LEGISLATION
TLU LEGISLATIVE PROPOSALS

This is to alert you to the on-going efforts of the Technology Law Unit in assisting OPCA in addressing the FBI's criminal legislative needs relating to computer and Internet investigations as well as responding to issues generated by various legislative proposals being submitted by members of Congress.

Attached are a series of documents which may be broken down into two (2) groups: 1) Amendments (with legal analysis) which the FBI supports to existing bills currently filed and under consideration, and; 2) Proposed amendments, the subject matter of which is not currently proposed bill. Some significant portions of these materials represent adaptations of proposals we support and which have been hammered out with CCIPS over the past several months. We understand from CCIPS that most of these proposals have been approved by the administration to be "shopped around" and CCIPS is generally aware of our providing technical drafting assistance and commentary to the staffs of members of Congress. This has been a time-intensive process which has absorbed significant TLU resources with regular assistance from ILU and is expected to continue until the end of the current legislative session.

b6-1
b7C-1

In addition, this is to alert you that TLU's [redacted] and [redacted] will be accompanying OPCA on Thursday, May 4, 2000 and Friday, May 5, 2000 to meet with Senator Hatch's staff and Senator DeWine's staff regarding high tech issues and FCC merger approval deadline issues (S.467) respectively.

Patrick W. Kelley
Deputy General Counsel

1 - Mr. Collingwood
1 [redacted]
1 - Mr. Steele
1 [redacted]

1 [redacted]
1 [redacted]
1 [redacted]
1 [redacted]

1 [redacted]
1 - 66F-HQ-C1299934

b6-1
b7C-1

Doc #2

PRIORITY OF MATTERS CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION.

1) Support funding for Technical Support Center and Regional Computer Forensic Laboratories. (Hatch)

2) "Tweaking" of language in the amending Pen Register/Trap and Trace Statute. (Kyl/Schumer)

3) "Tweaking" of language amending the Computer Fraud Statute. (Kyl/Schumer and Hatch)

4) Oppose Expansion of Secret Service 18 U.S.C. §1030 jurisdiction. (Hatch)

5/24/02 Release - Page 312

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

Support funding for Technical Support Center and Regional Computer Forensic Laboratories

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

1. "Support funding for Technical Support Center and Regional Computer Forensic Laboratories"

Support For Direct Funding to the FBI for the National Cyber-Crime Technical Support Center

The FBI strongly supports without reservation the provisions of section 109(a) of S.2448 as a necessary and critical element in United States' strategy to combat cyber-crime on a national and international level. The absence of adequate technical resources dedicated to the assistance of law enforcement in this arena undermines daily the investigative efforts of federal, state and local law enforcement officers dedicated to addressing the most troubling aspects of computers and the Internet such as child sexual exploitation, the dissemination of child pornography, the wholesale theft of intellectual property, the theft and disclosure of valuable trade secrets as well as countless more traditional crimes now being facilitated by the use of computers. The FBI's existing technical expertise, established with the FBI Laboratory Divisions's Engineering Research Facility, demonstrates the prudence in providing funding dedicated for these expressed purposes directly with the Director of the FBI as the most effective means of ensuring that such a facility is constructed and made operational with the least delay possible. Senate Bill 2448's approach is necessary, prudent and expeditious.

5/24/02 Release - Page 216

Support for Direct Funding to the FBI for the Creation of Regional Computer Forensic Laboratories

The FBI also supports without reservation the provisions of section 109(b) of S.2448 authorizing direct funding to the FBI for the express purpose of creating up to ten (10) Regional Computer Forensic Laboratories (RCFLs).

The FBI notes that, by separating funding for RCFLs under section 109(b) of S.2448 from State funding for task forces and other DOJ controlled investigative initiatives under 109(c), the bill implicitly acknowledges the difference between a true computer forensics capability which is and should be an objective, scientific function and a computer investigative capability[1], and have appropriately chosen to lodge responsibility for the former with the FBI through its laboratory division.

It is well known that the FBI Laboratory Division was instrumental in the development and realization of a Regional Computer Forensic Laboratory in San Diego, California at which federal, state and local law enforcement officers work side by side sharing both expertise and expensive equipment and software vital to the forensic recovery of often critical criminal evidence from computers and other digital media. The FBI Laboratory utilized its own financial resources to make the San Diego RCFL a reality and is providing extensive computer forensic training to state and local officers of that facility both at the FBI Academy and through computer industry recognized training programs. The FBI Laboratory Division now has some twenty (20) years experience in the science of computer forensics through its Computer Analysis Response Team (CART). With CART scheduled to expand from its current forensic complement of over 120 examiners to over 300 by the beginning of 2002 (which will continue to secure its place as the single largest computer forensic entity in the world), it only makes good sense to harness the FBI's expertise and knowledge of scientific method and forensic "best practices" as the means of jump starting a legitimate state and local computer forensic capability. The key to the success of the San Diego RCFL will be the key to success for future RCFLs, namely the ability to move quickly with a minimum of administrative expense, overhead or red tape. S.2448's direct funding appropriation make this possibility a reality.

For these and many other reasons, the FBI strongly supports the allocation of direct funding for RCFLs to the FBI.

---

[1] A computer investigative capability typically requires specially trained officers who are versed in Internet culture, Internet-based ponzi and othe fraud schemes as well as Internet chat vernacular enabling them to go on-line undercover to detect and investigate criminal behavior. In comparison, the focus of a computer forensics capability is the recovery, extraction, interpretation and stabilization of digital evidence, usually from digital storage media such as a computer hard drive seized as a result of a computer investigation. Computer forensic examiners typically are required to possess and master a far more detailed knowledge of electronics, computer hardware assembly and operation and software programing and operation than would be necessary for a computer investigator. A computer forensic facility is more detached from heat of the investigation and employs scientifically proven or accepted methodologies to recover either inculpatory or exculpatory evidence from a digital medium.

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

2. "Tweaking" of language in the amending Pen Register/Trap and Trace Statute. (Kyl/Schumer)

AMENDMENTS TO THE PEN REGISTER AND TRAP & TRACE STATUTE

It is suggested that the last sentence of the proposed modification of 18 U.S.C. § 3122(a) (and its legislative history) be changed to make clear that service of the new single, nation-wide court order is not required upon all providers in the communication chain if a single provider has access to all transmission data. The suggested change is:

"~~The order shall~~ Such order shall, upon service of the order, apply to any entity providing wire or electronic communications service in the United States whose assistance ~~is required to effectuate the order~~ may facilitate the execution of the order."

It is also suggested that the proposed revision to 3123 subsection (b) (1), new subparagraph (C) be changed for the reasons stated below in the proposed legislative history:

"(C) a description of --

(i) the technical nature of the communications to which the order applies, such as ~~including~~ the number or other identifier"

PROPOSED LEGISLATIVE HISTORY

Existing Subsection (C) is intended to require the identification of the "facility" to which the pen register or trap and trace is applied. Historically this was accomplished by identifying the telephone number of the targeted telephone, and if known the physical location of that telephone. With the increase in electronic communications via e-mail, chat sessions, instant Messaging, or telenet sessions, it may not always be possible to identify a static "facility." In cases of dynamic addressing of Internet accounts and telenet sessions for example, it is difficult to describe the facility through a static number. To address this, the statute should permit the applicants to describe the technical nature of the communications as a means of further identifying the facility to which the order applies. Examples might include the computer protocol or computer language utilized, or any dynamically assigned message identification number or code or part thereof.

The bill also inserts "routing, addressing" into the phrase "dialing and signaling information" in section 3121(c) and other provisions of the statute. The term "signaling" has historically been given an expansive reading to include, in the electronic communications world (e.g., e-mail), much of what would be "routing and addressing" and then some. It is stressed that the insertion and existence of "routing, addressing" into the statute is not intended to limit the interpretation of the term "signaling."

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

3. "Tweaking" of language amending the Computer Fraud and Abuse Act.

5/24/02 Release - Page 320

SUGGESTED ADDITIONAL AMENDMENTS TO THE COMPUTER FRAUD AND ABUSE ACT.

Counting Prior State Computer Crime Offenses:

A new § 1030(e)(10) would define conviction to include prior Federal juvenile adjudications for violations of § 1030. Given that the majority of States now have unauthorized computer access or similar computer crime statutes[2], it is suggested that the proposed new definition of conviction be further expanded to include prior State computer convictions. The

---

[2] Some 45 States have enacted statutes prohibiting, to varying degree, computer crime: AL Computer Crime Act, Code of Alabama, Sections 13A-8-100 to 13A-8-103; AK Statutes, Sections 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985, 11.46.990; AZ Revised Statues Annotated, Sections 13-2301(E), 13-2316; CA Penal Code, Section 502; CO Revised Statutes, Sections 18-5.5-101, 18-5.5-102; CT General Statutes, Sections 53a-250 to 53a-261, 52-570b; DE Code Annotated, Title 11, Sections 931-938; FL Computer Crimes Act, Florida Statutes Annotated, Sections 815.01 to 815.07; GA Computer Systems Protection Act, Georgia Codes Annotated, Sections 16-9-90 to 16-9-95; HI Revised Statutes, Sections 708-890 to 780-896; ID Code, Title 18, Chapter 22, Sections 18-2201, 18-2202; IL Annotated Statutes (Criminal Code), Sections 15-1, 16-9; IN Code, Sections 35-43-1-4, 35-43-2-3; IO Statutes, Sections 716A.1 to 716A.16; KS Statutes Annotated, Section 21-3755; KY Revised Statutes, Sections 434.840 to 434.860; LA Revised Statutes, Title 14, Subpart D. Computer Related Crimes, Sections 73.1 to 73.5; ME Revised Statutes Annotated, Chapter 15, Title 17-A, Section 357; MD Annotated Code, Article 27, Sections 45A and 146; MA General Laws, Chapter 266, Section 30; MI Statutes Annottated, Section 28.529(1)-(7); MN Statutes (Criminal Code), Sections 609.87 to 609.89; MI Code Annotated, Sections 97-45-1 to 97-45-13; MS Revised Statutes, Sections 569.093 to 569.099; MT Code Annotated, Sections 45-2-101, 45-6-310, 45-6-311; NE Revised Statutes, Article 13(p) Computers, Sections 28-1343 to 28-1348; NV Revised Statutes, Sections 205.473 to 205.477; NH Revised Statutes Annotated, Sections 638:16 to 638:19; NJ Statutes, Title 2C, Chapter 20, Sections 2C:20-1, 2C:20-23 to 2C:20-34, and Title 2A, Sections 2A:38A-1 to 2A:38A-3; NM Statutes Annotated, Criminal Offenses, Computer Crimes Act, Sections 30-16A-1 to 30-16A-4; NY Penal Law, Sections 155.00, 156.00 to 156.50, 165.15 subdiv. 10, 170.00, 175.00 NC General Statutes, Sections 14-453 to 14-457; ND Century Code, Sections 12.1-06.1-01 subsection 3, 12.1-06.1-08; OH Revised Code Annotated, Sections 2901.01, 2913.01, 2913.04, 2913.81; OK Computer Crimes Act, Oklahoma Session Laws, Title 21, Sections 1951-1956; OR Revised Statutes, Sections 164.125, 164.377; PA Consolidated Statutes Annotated, Section 3933; RI General Laws (Criminal Offenses), Sections 11-52-1 to 11-52-5 SC Code of Laws, Sections 16-16-10 to 16-16-40; SD Codified Laws, Sections 43-43B-1 to 43-43B-8; TN Code Annotated, Computer Crimes Act, Sections 39-3-1401 to 39-3-1406; TX Codes Annotated, Title 7, Chapter 33, Sections 33.01 to 33.05; UT Computer Fraud Act, Utah Code Annotated, Sections 76-6-701 to 76-6-704; VA Computer Crime Act, Code of Virginia, Sections 18.2-152.1 to 18.2-152.14; WA Revised Code Annotated, Sections 9A.48.100, 9A.52.010, 9A.52.110 to 9A.52.130 WI Statutes Annotated. Section 943.70; WY Statutes, Sections 6-3-501 to 6-3-505.

suggested additional language to the proposed bills' § 1030(e)(10) version would be:

> "; and
> (B) a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer."

Given the fact that most section 1030 offenders are juveniles and statistically more likely to first receive State juvenile adjudications, it is further recommended that the provision go even further than that outline above by including prior State juvenile adjudications.

Expanding the Definition of "loss" to Include Preventative Reconfiguration:

Another recommendation for the Hatch Bill is that the proposed definition of "loss" in Section 1030(e)(11) be made clearer to include the cost of plugging holes in computer defenses as a means of preventing future attacks---so called "preventative re-configuration/reprogramming." The new language could read:

> "(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, implementation of responsive security measures or reconfiguration reasonably calculated to prevent future damage, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;"

MATTER CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

4. Oppose Expansion of Secret Service 18 U.S.C. §1030 jurisdiction.

5/24/02 Release - Page 323

EXECUTIVE SUMMARY

Basis of Opposition to Amendment to Grant Concurrent Jurisdiction to the United States Secret Service in Section 1030 Offenses.

The proposed amendment to section 1030(d) of Title 18 would grant concurrent jurisdiction to the United States Secret Service (USSS) to investigate all crimes found in Section 1030.

In 1996, Congress specifically limited the Secret Service's authority to investigate crimes under 18 U.S.C. § 1030 to only those offenses under subsections (a)(2)(A) and (B), (a)(3), (a)(4), (a)(5) and (a)(6). The Senate Report accompanying the 1996 amendment explained that:

> [t]he new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

S. Rep. No. 357, 104th Cong., 2d Sess. 13 (1996).

Inherent in the 1996 changes was the recognition that the statute was being amended to reflect the respective investigative jurisdictional limits existing at that time. It was clear at that time, that the jurisdiction of the Secret Service, found at 18 U.S.C. § 3056, did not encompass the types of offenses described in Section 1030 (a)(1), (a)(2)(C), or (a)(7).[3] Given that there have been no additional grants of investigative jurisdiction to the USSS since that amendment, the current proposal to grant jurisdiction to the USSS is at best questionable. The theft of National Security information which is the type of information Section 1030(a)(1) was intended to address has never been the subject of USSS jurisdiction, nor should it be. In addition, the types of crimes contemplated by 1030(a)(2)(C) and (a)(7), as recognized by the legislative

---

[3] "Under the direction of the Secretary of the Treasury, the Secret Service is authorized to detect and arrest any person who violates –

(1) section 508, 509, 510, 871, or 879 of this title or, with respect to the Federal Deposit Insurance Corporation, Federal land banks, and Federal land bank associations, section 213, 216, 433, 493, 657, 709, 1006, 1007, 1011, 1013, 1014, 1907, or 1909 of this title;

(2) any of the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; or

(3) any of the laws of the United States relating to electronic fund transfer frauds, credit and debit card frauds, and false identification documents or devices; except that the authority conferred by this paragraph shall be exercised subject tot he agreement of the Attorney General and the Secretary of the Treasury and shall not affect the authority of any other Federal law enforcement agency with respect to those laws.

history, have traditionally been investigations solely in the province of the FBI.

The 1996 provision is an explicit effort by Congress to address the criminal offenses at issue through a division of labor primarily determined by investigative responsibility and expertise. Any reversion to the pre-1996 jurisdictional provisions raises serious issues and concerns about the utilization of resources. Concurrent jurisdiction will result in a duplication of efforts that will waste resources and will encourage independent investigations by separate agencies at the expense of coordinated joint efforts.

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION.

1. Cable Communications Act amendment.

EXECUTIVE SUMMARY
Cable Communications Policy Act Amendment

The Cable Communications Policy Act, passed in 1984 to regulate various aspects of the cable television industry, did not take into account the changes in technology that have occurred over the last fifteen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. This amendment clarifies that when a cable company acts as a telephone company or an Internet service provider, it must comply with the laws governing the interception and disclosure of wire and electronic communications just like any other telephone company or Internet service provider.

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER V-A--CABLE COMMUNICATIONS
PART IV--MISCELLANEOUS PROVISIONS

Section 551. Protection of subscriber privacy

(a) Notice to subscriber regarding personally identifiable information; definitions

(1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of--

(A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;

(B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

(C) the period during which such information will be maintained by the cable operator;

(D) the times and place at which the subscriber may have access to such information in accordance with subsection (d) of this section; and

(E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

(2) For purposes of this section, other than subsection (h) of this section--

(A) the term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons;

(B) the term "other service" includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and

(C) the term "cable operator" includes, in addition to persons within the definition of cable operator in section 522 of this title, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.

(b) Collection of personally identifiable information using cable system

(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

(2) A cable operator may use the cable system to collect such information in order to--

(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or

(B) detect unauthorized reception of cable communications.

(c) Disclosure of personally identifiable information

(1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

(2) A cable operator may disclose such information if the disclosure is--

(A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;

(B) subject to subsection (h) of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; ~~or~~

(C) a disclosure of the names and addresses of subscribers to any cable service or other service, if--

(i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and

(ii) the disclosure does not reveal, directly or indirectly, the--

(I) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or

(II) the nature of any transaction made by the subscriber over the cable system of the cable operator; or

(D) required under chapters 119, 121, or 206 of title 18, United States Code. Such disclosure shall not include records revealing customer cable television viewing activity. For purposes of this section, "customer cable television viewing activity" shall mean the cable customer viewing habits of operator-selected, pre-

scheduled video and audio presentations.

(d) Subscriber access to information

A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.

(e) Destruction of information

A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) of this section or pursuant to a court order.

(f) Civil action in United States district court; damages; attorney's fees and costs; nonexclusive nature of remedy

(1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(B) punitive damages; and

(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

(3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

(g) Regulation by States or franchising authorities

Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.

(h) Disclosure of information to governmental entity pursuant to court order

Except as provided in subsection (c)(2)(D), a ~~A~~ governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order--

(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

PROPOSED LEGISLATIVE HISTORY FOR AMENDMENTS TO THE CABLE COMMUNICATIONS POLICY ACT

The Cable Communications Policy Act currently establishes two different sets of rules regarding privacy protection and disclosure to law enforcement: one governing cable service ("Cable Act") (47 U.S.C. §551), and the other applying to the use of telephone service and Internet access, (the wiretap statute (18 U.S.C. §2510 et seq.), the Electronic Communications Policy Act ("ECPA") (18 U.S.C. §2701 et seq.), and the pen register and trap and trace statute (18 U.S.C. §3121 et seq.). Yet today, unlike in 1984 when Congress passed the Cable Communications Policy Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. The rules governing law enforcement access to the records of communication service providers' customers, however, should not depend on whether the customer has chosen to use a cable company or a more traditional type of provider for his telephone or Internet service. Congress believes that cable companies offering such services should comply with court orders and other legal process permitted under the wiretap statute, ECPA, and the pen register and trap and trace statute with respect to their telephone and Internet customers.

In recent years, however, cable companies have increasingly balked at complying with such process, noting the seeming inconsistency of these statutes with their duty of nondisclosure (except under stringent limits) under the Cable Communications Policy Act. See In re Application of United States, 36 F. Supp. 2d __ (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) against cable company providing Internet service). These complications have at times delayed or frustrated investigations.

In addition, section 551 is flawed because it permits law enforcement to obtain information only when that information constitutes evidence of an offense. In some cases, however, the information sought from a service provider is not evidence of a crime, even though it helps to solve one. For example, law enforcement officials may try to arrest a fugitive who is accessing his e-mail account from a remote location, and they need to obtain information from

the cable company that shows from what location he is accessing that account. Moreover, whether law enforcement can obtain a court order to obtain such information should not depend on whether the fugitive has chosen to connect to the Internet using a cable company instead of a traditional Internet service provider.

Accordingly, the amendment inserts a new subsection 551(c)(2)(D) to confirm that cable companies, like other providers, remain subject to ECPA, the wiretap statute, and the trap and trace statute with respect to the provision of telephone and Internet services, notwithstanding section 551. The definition of "customer cable television viewing activity" is intended to exclude from disclosure under chapters 119, 121, or 206 of title 18 of the United States Code traditional cable and broadcast television video/audio presentations Unlike Internet video presentations, the subject content and timing of which are selected by the cable customer, the selection and timing of television presentations are controlled by the operator. The disclosure exclusion is not intended to encompass or prohibit the disclosure by an operator of records or information relating to television presentations which are re-transmitted through the Internet. Records relating to such re-transmissions would be treated like all other Internet-related records under chapters 119, 121, or 206 of title 18. The amendment, however, is intended to preserve the Cable Act's primacy with respect to records revealing what ordinary cable television programing a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can compel disclosure under ECPA only those customer records relating to Internet service.

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

2. Privacy Protection Act amendment

5/24/02 Release - Page 333

EXECUTIVE SUMMARY

Necessary Amendments to the Privacy Protection Act - 42 U.S.C. § 2000aa, *et seq.*

The Privacy Protection Act (PPA) prohibits law enforcement from searching for or seizing work product materials or documentary materials possessed by a person in connection with a purpose to disseminate them to the public in a newspaper, book, broadcast, or other similar form of public communication. Originally adopted to prevent the search of third party news-gathers in traditional media (e.g., newspaper press rooms, tv editor offices), the PPA has generated unforseen obstacles for law enforcement when applied to the search of a criminal's personal computers if the computers coincidentally are being used for web site publishing. A scenario frequently encountered by law enforcement involves the seizure of a computer used to disseminate child pornography which may coincidentally also control the e-mail and/or websites of the suspect and third parties. Because of the size of modern personal computer hard drives today, most computers cannot effectively be searched on scene, but are usually seized first, then searched later in a computer forensic environment as expressly provided for by a magistrate issuing the warrant. Unfortunately, such a practice creates a dilemma for investigators who may learn later during the examination process that potential third party news gatherer material may exist on the computer system. The realization may be too late as the PPA prohibits both search and seizure of such material.

Amendments detailed herein would carve out a reasonable exception to the Act when the search or seizure of work product materials or documentary materials is "incidental to" the search or seizure of other evidence relevant to a crime. Thus, the seizure of a computer hard drive of non-defendant third party for evidence of child pornography would not be prohibited merely because the same hard drive contained work product or other documentary material prohibited by the PPA.

[redline strikeout version of amendments to the Privacy Protection Act]

UNITED STATES CODE ANNOTATED
TITLE 42. THE PUBLIC HEALTH AND WELFARE
CHAPTER 21A--PRIVACY PROTECTION
SUBCHAPTER I--FIRST AMENDMENT PRIVACY PROTECTION
PART A--UNLAWFUL ACTS

Section 2000aa. Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses

(a) Work product materials

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275 or 2277 of this title, or section 783 of Title 50, or if the offense involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, the sexual exploitation of children, or the sale or purchase of children under section 2251, 2251A, 2252, or 2252A of Title 18); ~~or~~

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.; or

(3) the seizure or examination of work product materials is incidental to the execution of

an otherwise lawful search or seizure.

(b) Other documents

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275, or 2277 of this title, or section 783 of Title 50, or if the offense involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, the sexual exploitation of children, or the sale or purchase of children under section 2251, 2251A, 2252, or 2252A of Title 18);

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being;

(3) there is reason to believe that the giving of notice pursuant to a subpoena duces tecum would result in the destruction, alteration, or concealment of such materials; ~~or~~

(4) such materials have not been produced in response to a court order directing compliance with a subpoena duces tecum, and--

(A) all appellate remedies have been exhausted; or

(B) there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpoena would threaten the interests of justice~~;~~ or

(5) the seizure or examination of documentary materials is incidental to the execution of an otherwise lawful search or seizure.

(c) Objections to court ordered subpoenas; affidavits

In the event a search warrant is sought pursuant to paragraph (4)(B) of subsection (b) of this section, the person possessing the materials shall be afforded adequate opportunity to submit an affidavit setting forth the basis for any contention that the materials sought are not subject to seizure.

PROPOSED LEGISLATIVE HISTORY FOR AMENDMENTS TO THE PRIVACY PROTECTION ACT

The Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. § 2000aa, et seq., makes it unlawful for local, state, or federal law enforcement authorities to "search for or seize any *work product materials*" or any "*documentary materials* ... possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. § 2000aa(a), (b). The statute defines "work product materials" as materials prepared or possessed in anticipation of communicating such materials to the public, except if the materials constitute contraband or the fruits or instrumentalities of crime. Id. § 2000aa-7(b). "Documentary materials," on the other hand, consist of materials upon which information is recorded, once again with the exception of contraband and the fruits or instrumentalities of crime. Id. § 2000aa-7(a). Thus, other than for the exceptions, the PPA effectively imposes a "no-search" rule on work product materials and a "subpoena-first" rule on documentary materials held by third parties who plan to use them to communicate to the public. Although the statute appears reasonable on its face, its application in the current electronic environment has inadvertently shielded criminal activities from legitimate law enforcement investigations, such efforts to arrest and prosecute those who distribute child pornography over the Internet.

(a) Intent of the PPA

Congress passed the PPA in response to the Supreme Court's decision in Zurcher v. Stanford Daily, 436 U.S. 537 (1978). In Zurcher, the Supreme Court upheld a police search, pursuant to a valid search warrant, of the offices of The Stanford Daily newspaper for photographs taken at the scene of a crime. The Court rejected the newspaper's claim that search warrants could not be used to recover evidence from those engaging in First Amendment-protected activities. Id. at 565-567. The Court also held that law enforcement officers could use search warrants to recover evidence from innocent third parties. Id. at 555 ("state's interest in enforcing the criminal law and recovering evidence is the same whether the third party is culpable or not"). The Court concluded, therefore, that "the critical element in a reasonable search is not that the owner of the property is suspected of a crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." Id. at 556.

In response to the Court's ruling, Congress passed the PPA. Congress intended to restrict searches for mere evidence of crime held by *innocent third parties* who were engaged in First Amendment-protected activities — evidence that law enforcement officials might otherwise obtain through less intrusive means, such as by issuing a subpoena. The purpose of restricting law enforcement in this fashion, of course, was to protect the confidentiality of non-evidentiary files also held by this special group of innocent third parties — both the drafts of articles not yet published and the research and other supporting information (e.g., notes and interviews) which they never intended to publish. Thus, the PPA protects an author or publisher (like The Stanford Daily) — who is not a suspect in the investigation — from law enforcement attempts to search

5/24/02 Release - Page 338

through his or her work product or documentary materials in order to find and seize evidence. To preserve the confidentiality of these designated materials, the PPA instructs investigators not to search for the evidence at all, but to compel the innocent third parties to find and produce it themselves. This goal of Congress remains unchanged, and our amendments do not alter this protection for innocent third parties.

Congress never intended, however, to protect criminals from court-authorized searches, and the legislative history to the PPA is replete with statements to this effect. For example, the Senate Judiciary Committee Report stated that the purpose of the PPA is to "limit searches for materials held by persons involved in First Amendment activities *who are themselves not suspected* of participation in the criminal activity for which the materials are sought." S. Rep. No. 96-874, 96th Cong., 2d Sess. 11 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3957 (emphasis added). Moreover, the Committee Report stated that the intention in enacting the PPA was "not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation." Id. Indeed, the language of the statute itself allows searches and seizures of any person who "has committed or is committing the criminal offense to which the materials relate." 42 U.S.C.A. § 2000aa(a)(1), (b)(1). Plainly, Congress had no desire to inhibit law enforcement investigators that need to search the premises of a suspected wrongdoer.

(b) The problem of commingling of protected documents and evidence

Because Congress enacted this statute before the widespread proliferation of computers, it could not fully consider the problem raised by the commingling of protected information and contraband. Although commingling can, of course, occur with paper records — for example, if a reporter engaging in tax fraud placed a copy of the fraudulent tax return in a filing cabinet with his or her work-related notes — such commingling never presented a significant problem for two reasons. First, the statute applied only to members of the traditional media, a limited group not usually associated with committing crimes. Second, when searching for paper records, investigators can generally examine records on site and then seize only those records that are the subject of their warrant. Thus, investigators can avoid violating the PPA by not "searching for" or "seizing" any protected material since they do not need to carry away anything but the object of their search.[4]

With the widespread use of computers and the Internet, however, both of these limiting factors have disappeared. First, every computer user has become a potential publisher. For example, a single computer can provide (1) an electronic "bulletin board" for the posting of news items by individuals using the Internet; (2) user accounts where private individuals can store drafts of news items that they intend to post on the "bulletin board"; and (3) a website from

---

[4] Of course, investigators may briefly isolate or possess protected material during the execution of the warrant, but such possession occurs during the execution of every search warrant and does not constitute a seizure.

which anyone with access to the Internet could view or download child pornography. Although the second category of data arguably constitutes "work product" under the PPA,[5] law enforcement officials plainly have the duty to search for and seize the third category of data.

Second, potential liability under the PPA may arise for law enforcement officials in such a scenario because it has become both unreasonable and impractical, and in some instances technically impossible to search for and seize the contraband without simultaneously seizing protected material. In the new electronic environment, where computer systems with gigabytes of storage have become ubiquitous, law enforcement agents generally cannot extract legally seizable evidence from commingled protected material without actually seizing, at least temporarily, those protected materials, or, perhaps more intrusively, without moving into and occupying the search premises for extended durations. Because of the volume of data to be searched or because of technical concerns (e.g. encryption), law enforcement agents must very often remove the seized computer or an exact copy of all the data to a laboratory for analysis.

Moreover, liability may attach in such cases because the prohibition on searching for or seizing materials is stated in the disjunctive: violations may lie *either* for searching for *or* seizing such materials. Thus even a temporary seizure or examination may result in liability, despite the fact that such a PPA violation lies far outside the scope of the issues raised by the Zurcher decision. Zurcher involved a search of a newspaper office, and the warrant was drawn to intentionally seize photographs that had been made in contemplation of publication. The PPA, designed to address the Zurcher decision, accordingly should deter law enforcement from intentionally *searching for* evidentiary materials in the possession of innocent third parties engaged in information dissemination. But making unlawful the reasonable but incidental seizure of PPA-protected materials pursuant to an otherwise lawful search or seizure carries no similar deterrent effect, and it contravenes the clearly stated intent of Congress to neither shield criminals nor unduly hinder law enforcement efforts.

(c) Problems faced by law enforcement

The potential — and unpredictable — liability inadvertently created by the PPA has inhibited the investigation and prosecution of crimes committed using computers. For example, individuals have used computers to distribute child pornography, copyrighted software, and stolen credit card numbers over ordinary phone lines and the Internet. Some of these individuals have attempted to use the PPA to shield their illegal activities by intentionally storing PPA-protected materials on the same storage devices that they use for their illegal activities. Indeed, law enforcement agents have encountered individuals using computers for illegal activities that have posted the following message on their sign-on screens:

---

[5] No court has yet held that an electronic message, posted for viewing by the general public by way of a Bulletin Board System or the Internet, constitutes a "similar form of public communication" to newspapers, books, and broadcasts under the PPA. Although the instant amendments to the PPA do not opine on this subject, a court might make this ruling if presented with the right facts.

NOTICE TO LAW ENFORCEMENT AGENTS:

> The owners and users of this system are exercising First Amendment Rights. . . . Some material on this system is in preparation for public dissemination and is "work product material" protected under the First Amendment Privacy Protection Act of 1980 . . . . Each and every person who has such "work product material" stored on this system is entitled to recover at least minimum damages of $1000 *plus all legal expenses* . . . . While the agency you work for *might* pay your legal fees and judgments against you, why take chances?

The language "[s]ome material on this system" is extremely significant. It is seldom the case that a computer is used solely for illegal purposes such as the distribution of contraband. Were this the case, the computer and the evidence it contains could be seized without regard to the PPA, since contraband is specifically excluded from the definitions of work product and documentary materials. 42 U.S.C. § 2000aa-7(a) (defining "documentary materials"); 42 U.S.C. § 2000aa-7(b) (defining "work product materials"). In most cases, only certain portions of a website or electronic bulletin board will be set aside for illegal activities, while other portions are used for completely legal activities such as the legitimate distribution of information. As the quoted language makes clear, however, criminals are well aware that under the PPA, protected materials can be used to shield contraband from search and seizure. Congress, of course, never intended to shield contraband when it enacted the PPA.

Moreover, in addition to exposing law enforcement to unintended liability, the PPA, as it stands, creates unnecessary problems during the execution of warrants, problems that potentially harm the health and safety of the public. In 1999, for example, Special Agents of the Federal Bureau of Investigation uncovered a system of computers used to provide child pornography to anyone with access to the Internet. These computers, however, also provided Internet accounts to third parties, many of whom did not know about the illegal activities of the computers' operators. These unrelated accounts may have contained material protected by the PPA. The investigators determined that it would be impossible to search the computers on site while at the same time allowing the computers to continue to operate. Thus, in an effort to reduce their potential liability under the PPA for seizing the third party accounts, the investigators decided to obtain a search warrant authorizing them only to *copy* the computers' stored data and allow the computers to continue to operate. This, of course, had the effect of allowing the child pornography to remain accessible to the public — and possibly even allowing the pornographers or their confederates to copy the images to an unknown computer — while computer experts reviewed the data to segregate the illegal files. Congress never intended to hamper law enforcement efforts in this way.

(d) The solution

While the PPA must be amended so that it does not shield child pornographers,

copyright infringers, and other criminals, such amendments should not inhibit those activities that the PPA was designed to protect. Indeed, the importance of protecting the confidentiality of these sensitive materials remains as great today as it has ever been. Thus, the law should limit the intrusiveness of government searches but should not unnecessarily hinder law enforcement's efforts to enforce the criminal laws. The language of this bill achieves this delicate balance between important values.

The bill's new provisions, Title 42, United States Code, sections 2000aa(a)(3) and 2000aa(b)(5), make it clear that law enforcement agents may still search for or seize contraband, instrumentalities, and evidence not protected by the PPA, even if work product or documentary material may incidentally be examined or seized during a search. It is important to note, however, that where an innocent third party possesses the items sought, and if the items sought are commingled with work product or documentary materials, existing regulations already require investigators to avoid using a search warrant or subpoena where less intrusive means are appropriate. See, e.g., 28 C.F.R. 50.10 (requiring Justice Department officials to use all other means available to obtain information before issuing subpoena to member of the news media); 28 C.F.R. §59.4(a) and 28 C.F.R. §59.4(c)(1)(11) (in determining whether to use a warrant or subpoena to obtain documentary materials, an attorney for the government should consider whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect). Thus, even though the PPA would not restrict such incidental seizures, the Committee believes that government agents will need to consider what method is proper for obtaining the evidence based upon the facts of the case at hand.

Although these amendments to the PPA address the problem of incidental searches or seizures, these changes do not in any way alter the statute's effect in cases like Zurcher. The law enforcement officials who searched The Stanford Daily — which was not involved in any criminal activity — sought the very documentary materials that the PPA now protects. These materials, therefore, were not "incidental" to the search, and they therefore would not meet the exception found in the new amendments. Thus, even under the new law, when law enforcement agents encounter a situation like that in the Zurcher case, they will still have to use a subpoena as the original PPA directed.

But in other cases, where the search is "otherwise lawful" (i.e. the object of the search is something other than "work product" or "documentary" materials), these amendments to the PPA will ensure that investigators can carry out their duties, even when PPA-protected materials may be commingled with seizable ones. The amendments' use of the term "incidental" clearly prohibits situations in which protected materials are the object of the search. The term "incidental," which appears in other statutes (see, e.g., 18 U.S.C. §2510(17)), means something which is "occurring or likely to occur at the same time or as a consequence."[6] Accordingly, in order to be "incidental" within the intent of this provision, any search or seizure of protected materials would have to be a concomitant consequence of a search for materials not protected by

---

[6] The American Heritage Dictionary, Second College Edition (1989).

the PPA.[7]

Additionally, of course, the link between the incidental items and the lawful object of the search or seizure must be reasonable on the facts of the case. This requirement that such a search be reasonable is directly analogous to the Fourth Amendment requirement of reasonableness both in the scope of a search warrant and in its execution. See O'Connor v. Ortega, 480 U.S. 709, 726 (1987); United States v. Henson, 848 F.2d 1374 (6th Cir. 1988); United States v. Tamura, 694 F.2d 591 (9th Cir. 1982). Cases that have nothing to do with the PPA have caused courts to wrestle with whether, under all the facts and circumstances, seizing certain incidental materials was sufficiently reasonable to meet the Fourth Amendment standard. Thus, the amendments do not, by any means, invite law enforcement to use "an otherwise lawful" search as a pretext for an unreasonable rummaging of other documents — whether protected by the PPA or not. On the contrary, this new exception to the PPA will allow courts to apply existing and well-established Fourth Amendment jurisprudence in analyzing the analogous question of whether any incidental search or seizure of PPA-protected materials has been reasonable under the circumstances.

[7] This provision does not, of course, require that the incidental seizure of protected materials be inadvertent; law enforcement officers may knowingly seize protected materials where such seizure is incidental to a lawful search.

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

4. Clean Hands Exception to the Statutory Suppression of Intercepted Communications.

EXECUTIVE SUMMARY

Amendments Creating a "Clean Hands" Exception to Provisions Statutorily Mandating the Suppression of Illegally Intercepted Communications.

The accompanying amendments would create a "clean hands" exception to the statutory suppression mandates of 18 U.S.C. §2515 governing the use and introduction of illegally intercepted wire or oral communications. The proposal would allow for the use in a criminal investigation and the introduction into evidence in criminal matters of communications otherwise illegally intercepted by persons other than law enforcement, ONLY if law enforcement was neither directly or indirectly involved in its acquisition. Not unlike the rationale supporting the "good faith" exception to the Fourth Amendment's exclusionary remedies, implicit in the proposed amendment is the determination that the truth-finding functions of the criminal process are paramount when there is little or no law enforcement deterrence effect achievable. In contrast to existing law which prohibits all use, the proposed amendment would allow the introduction of such evidence both when it is inculpatory or exculpatory in nature.

"CLEAN HANDS" EXCEPTION TO STATUTORY EXCLUSIONARY RULE

(Exclusive of Other Substantive Amendments)

Section 2515. Prohibition of use as evidence of intercepted wire or oral communications

(a) Except as provided in subsection (b), ~~Whenever~~ whenever any wire, or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

(b) Subsection (a) shall not apply to the disclosure or use, in a criminal investigation, proceeding, hearing or trial, or before a grand jury, of the contents of a communication, or evidence derived therefrom—

(1) intercepted by a person not acting under color of law, provided that the party seeking to disclose or use the contents did not participate directly or indirectly in the interception, or

(2) against a person alleged to have intercepted the communication, or participated in its interception, in violation of this chapter.

Section 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter (or under circumstances described in section 2515(b)), has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter (or under circumstances described in section 2515(b)), has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political

subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

Section 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing

probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual

operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (8)(d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections

(1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court,

department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval;

except that no suppression may be ordered under the circumstances described in section 2515(b). Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for non-constitutional violations of this chapter involving such communications.

"CLEAN HANDS" EXCEPTION PROPOSED LEGISLATIVE HISTORY

Inapplicability of 18 U.S.C. §2515 statutory exclusion and non-use of certain "clean hands" good faith disclosures

This proposed change makes a carefully limited amendment of 18 U.S.C. §2515, the statutory exclusionary rule for violations of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, so as clearly to exempt two situations: (1) those in which private individuals illegally intercept or record a communication, but the recording later comes into the possession of a party in a criminal trial, who then wishes of introduce it; and (2) those in which an individual violates chapter 119 (*e.g.*, by engaging in an illegal wiretap) and the government thereafter seeks of use the communication to prosecute that violator.

At present, appellate decisions are in apparent conflict over whether section 2515 precludes the use of communications in the first category described above. Under one possible interpretation of section 2515, if a private individual consensually records a conversation in aid of an illegal activity, or illegally records a conversation between other parties without their consent, the contents of such recordings are not admissible in a criminal trial or hearing even if the government had no role in having the evidence recorded and only acquired it, through lawful means, at a later date. This situation occurs because, under 18 U.S.C. §2511(2)(d), a consenting party, not acting under color of law, may record only if the recording is for a non-criminal or non-tortious purpose. Thus, if the payer of a bribe secretly records the transaction in which he or she pays the bribe of an official, and the government later obtains the recording and seeks of use it against the official of prove the bribe, section 2515 arguably precludes such use. One appellate court has so held. United States v. Vest, 813 F.2d 477 (1st Cir. 1987).

By contrast, another appellate court has held that section 2515 does not bar the government from using recordings made by an illegal gambling business (of bets placed by telephone) to prevent disagreements with bettors over the amounts of their bets. United States v. Underhill, 813 F.2d 105 (6th Cir.), cert. denied, 484 U.S. 821, 846 (1987). While the court in Vest acknowledged that no deterrent purpose would be served by suppression because the government played no role in the illegal recording, it relied on the fact that further disclosure in court of the contents would magnify the original privacy violation. The court in Underhill, on the other hand, relied on clear legislative history indicating that Congress, despite the facial breadth of section 2515, did not intend to permit lawbreakers to immunize themselves from prosecution by the very criminal purposes that made the recordings illegal.

The same disagreement among circuit courts exists regarding the admissibility of recordings made by private actors intercepting communications without the consent of any of the parties. In one case, a court barred the use before a grand jury of such illegally intercepted communications. See In re Grand Jury, 111 F.3d 1066 (3d Cir. 1997). By contrast, where a wife secretly installed a recording device to intercept her husband's conversations with other persons, the Sixth Circuit concluded that section 2515 did not bar the use of the contents of those

communications in a prosecution of the husband, given the government's lack of involvement in the original interception. See United States v. Murdock, 63 F.3d 1391 (6th Cir. 1995).

Whether or not Vest and In re Grand Jury were correctly decided under the existing statutory provision, an exemption should be created under section 2515 for that narrow class of cases in which the government lawfully obtains illegal recordings made by private parties and seeks to use them as evidence in a criminal investigation, proceeding, hearing or trial, or before a grand jury. The truth-seeking function of a criminal proceeding is of paramount importance. In the absence of any deterrent purpose to be served by exclusion, this truth-seeking function should prevail over the concern that disclosure in the criminal proceeding would somehow exacerbate the original illegal recording.

Conversely, if evidence contained in an illegally intercepted recording tends to exculpate a defendant, that defendant should be entitled to introduce the evidence so long as he did not participate in the interception in any way. The instant amendment thus reflects the belief that a private violation of the statute should not trigger the severe result of exclusion of otherwise probative evidence in a criminal case (just as the Fourth Amendment, of course, does not apply to non-governmental searches and seizures[8]). Accordingly, this section would amend section 2515 to expressly exempt such disclosures from its purview.

In addition, the amendment would also clarify that illegal intercepts made be used for the limited purpose of prosecuting the individual who conducted the illegal interception. In one recent case, United States v. Grice, 37 F. Supp. 2d 428 (D.S.C. 1998), an employee of a county sheriff's department illegally intercepted conversations between two prisoners and their attorneys. When the United States sought to use the recording of prosecute that violation, the district court ruled the evidence inadmissible. The amendment would permit such use for the purpose of prosecuting the violator of chapter 119. Conforming amendments are also made of subsections (1) and (2) of section 2517 and subsection 2518(10)(a) .

[8] The history of section 2515's original enactment makes clear that Congress intended that it embody existing Fourth Amendment standards. See S. Rep. No. 1097, 90th Cong. 2d Sess., reprinted in 1968 U.S.C.C.A.N. 2112, 2185 (no intention "of press the scope of the suppression role beyond present search and seizure law").

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

5. Emergency Pen Register/Trap and Trace authority at field level.

EXECUTIVE SUMMARY

Amendment Creating Emergency Pen Register/Trap & Trace Authority for US Attorneys and Top Law Enforcement.

Under current law, 18 U.S.C. § 3125(a), an emergency pen register or trap & trace may be authorized only by certain high level DOJ officials or "any investigative or law enforcement officer specially designated by the Attorney General" or, in cases involving the States, the equivalent of the County District Attorney. Emergency pen register or trap & trace orders are authorized under section 3125(a) only when there exists an immediate danger of death or serious bodily injury to any person, or where there are conspiratorial activities characteristic of organized crime. And this bill will add two other emergency circumstances to bring the pen register statute in relative parallel with the wiretap emergency provisions and to acknowledge that attacks on certain government or public computer infrastructure could seriously endanger the public health or safety.

Even in emergency situation, a court order ratifying the use of the pen register or trap & trace must be sought and obtained within 48 hours. Since the current statute authorizes the issuance of an emergency pen register at the State level by any County District Attorney, it has been argued that the current restrictions on emergency deployment by Federal authorities are, by comparison, incongruous, unnecessarily restrictive, cumbersome and time consuming. Based upon law enforcement's experience, the problem is especially acute in dynamic computer investigations where time is frequently of the essence. The proposed amendment would, in addition to the class of DOJ officials currently authorized to issue emergency pen registers or implement trap & trace, statutorily authorized the issuance of emergency implementation upon the request of either a "United States Attorney or the principal supervising law enforcement officer of any Federal criminal investigative agency."

Designating the United States Attorney or the principal supervising law enforcement officer with the authority to conduct a pen register or trap and trace in an emergency situation vests authority with the official who is in the best position to assess the need and propriety of use when the passing of mere minutes may mean the loss of valuable information, for example, in an ongoing computer attack. At the same time, this express designation will continue to assure the consistent administration of law enforcement policy on the use of pen registers and trap and trace devices by retaining centralized responsibility for approving emergency use in a limited number of identifiable and politically accountable officials.[9]

---

[9] S. Rep. No. 1097 90th Cong. 2d Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185 (approval level for wiretap applications).

5/24/02 Release - Page 356

EXPEDITING EMERGENCY PEN REGISTER AND TRAP & TRACE IMPLEMENTATION

(Exclusive of any other Amendments)

Section 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, ~~any investigative or law enforcement officer, specially designated by~~ the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, ~~or~~ any Deputy Assistant Attorney General, any United States Attorney or the principal supervising law enforcement officer of any Federal criminal investigative agency, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

MATTER NOT CONTAINED
IN BILLS CURRENTLY UNDER CONSIDERATION

5. Title III Wiretap Exception for the Interception of Unauthorized Computer Trespassers Only upon the Written Request of the Owner/operator of the Computer System.

COMPUTER TRESPASSER INTERCEPTION EXCEPTION

(Irrespective of other Amendments)

[18 U.S.C. §2511]

(2)(a)(iii) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser, provided that-

(A) the owner or operator of the protected computer authorizes in writing the interception of the computer trespasser's communications on the protected computer;

(B) the person acting under color of law is lawfully engaged in an ongoing investigation;

(C) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the ongoing investigation; and

(D) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

[18 U.S.C. §2510]

(19) "computer trespasser" means a person who has no reasonable expectation of privacy in any communication transmitted to, through, or from a protected computer because such person is accessing the protected computer without authorization.

PROPOSED LEGISLATIVE HISTORY FOR COMPUTER TRESPASSER INTERCEPTION EXCEPTION

The amendment allows, but does not require, owners and operators of either public or private electronic or wire communication services to authorize law enforcement to intercept the communications/transmissions of a party, person or computer who the owner or operator of that service has first determined and certified is an unauthorized user on that computer system or network. The amendment is premised upon and acknowledges the legal conclusion that unauthorized users (e.g., hackers), not unlike burglars who've illegally entered a private dwelling, do not possess an expectation of privacy in their unauthorized communications which society deems reasonable or which should be protected by statute. The amendment imposes the formal requirement that the consent of the owner or operator be both prior and written so as to deter casual utilization of the exception.

(01/26/1998)

66-1
67C-1 [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 07/21/2000 Date: 07/17/2000

To: Director's Office Attn: Deputy Director's Office
Mr. Pickard
Laboratory Division Dr. Kerr
Office of General Counsel Mr. Parkinson

From: Director's Office
Office of Public and Congressional Affairs
Congressional Affairs Office
Contact: SSA [redacted] Ext. [redacted] 66-1 67C-1

Approved By: Pickard Thomas J
Kerr Donald M
Parkinson Larry R
Collingwood John E
[redacted] 66-1 67C-1

Drafted By: [redacted]

Case ID #: 62C-HQ-1077728 (Pending)

Title: ACTION MEMORANDUM:
HOUSE JUDICIARY COMMITTEE;
CONSTITUTION SUBCOMMITTEE;
HEARING ON "FOURTH AMENDMENT ISSUES RAISED BY THE FBI'S 'CARNIVORE' PROGRAM"
07/24/2000

Synopsis: The Constitution Subcommittee of the will conduct a hearing on Monday, 07/24/2000, at 1:00 PM, in Room 2141 of the Rayburn House Office Building. The purpose of the hearing is to examine "Fourth Amendment issues raised by the FBI's 'Carnivore' program." Consequently, the Subcommittee has requested that Laboratory Division Director Dr. Donald M. Kerr and General Counsel Larry R. Parkinson appear on behalf of the FBI.

Details: The Constitution Subcommittee will conduct a hearing to examine Fourth Amendment issues raised by "Carnivore." The Subcommittee has preliminarily advised that the hearing will be composed of two panels. The first panel will have witnesses from the U.S. Department of Justice (DOJ), to include the FBI. The second panel will be composed of individuals from private industry and Internet privacy groups. It is anticipated that Deputy Assistant Attorney General Kevin DiGregory, as well as David Green from CCIPS, will represent the Department. The specific private sector witnesses have not yet been determined.

DOC #3

To: Director's Office From: Director's Office
of Public and Congressional Affairs
Re: 62C-HQ-1077728, 07/17/2000

The Subcommittee has requested that the Laboratory Division and the Office of the General Counsel provide a written statement for the official record which the witnesses may summarize for the Subcommittee. The written statement must also be provided to the Subcommittee on a computer disk or through email. These items must be provided to the Subcommittee no later than Friday, 07/21/2000. A letter of invitation from the Subcommittee has not yet been received.

LEAD(s):

Set Lead 1:

DIRECTOR'S OFFICE

AT WASHINGTON, DC

It is requested that the Deputy Director approve Dr. Kerr and Mr. Parkinson's participation as witnesses at captioned hearing.

APPROVE _____
DISAPPROVE _____
SEE ME _____

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

It is requested that the Laboratory Division prepare testimony, with assistance from the Office of General Counsel, for Dr. Kerr and provide it to SSA [redacted] Room [redacted] Extension [redacted] by COB 07/19/2000, in order that it may be transmitted to DOJ for clearance and then to the Subcommittee in a timely fashion. b6-1 b7C-1

5/24/02 Release - Page 362

To: Director's Office From: Director's Office
of Public and Congressional Affairs
Re: 62C-HQ-1077728, 07/17/2000

Set Lead 3:

GENERAL COUNSEL

AT WASHINGTON, DC

It is requested that the Office of General Counsel assist the Laboratory Division, as needed, in the preparation of testimony for captioned hearing.

Set Lead 4:

OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS,
CONGRESSIONAL AFFAIRS OFFICE

AT WASHINGTON, DC

The Congressional Affairs Office will coordinate the appearances of Dr. Kerr and Mr. Parkinson before the Subcommittee; the approval of the testimony from the Deputy Director's Office; and the veting of the testimony by DOJ.

b6-1
b7C-1

1 - Mr. Pickard
1 - Dr. Kerr
1 - Mr. Parkinson
1 - Mr. Allen
1 - [redacted]
JCS
(13)

1 - Mr. Bucknam
1 - [redacted]
1 - [redacted]

1 - Mr. Collingwood
1 - [redacted]
1 - [redacted]
1 - CAO File Copy

♦♦

5/24/02 Release - Page 363

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #4 FROM THE OGC/FLU FILE (PAGES 162 & 163)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #4 (Pages 364-365)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

The New York Times

DATE: 7-18-00
PAGE: A-1

PROPOSAL OFFERS SURVEILLANCE RULES FOR THE INTERNET

INTERCEPTION OF E-MAIL

White House Tries to Balance Rights of Computer Users and Law Enforcement

By STEPHEN LABATON
with MATT RICHTEL

WASHINGTON, July 17 — The White House said today that it would propose legislation to set legal requirements for surveillance in cyberspace by law enforcement authorities similar in some ways to those for telephone wiretaps.

Privacy advocates and civil liberties groups welcomed some aspects of the proposal but said they remained alarmed about a new F.B.I. computer system that searches and intercepts private e-mail and can easily capture communications of people not suspected of crimes.

The legislative proposal was made as the administration also announced today that it had eased export controls on encryption technology, making it significantly easier for American companies to sell software products to the European Union and eight other trading partners that can be used to keep computer data and communications secure.

Both the electronic surveillance proposal and the export control changes are part of a broader policy outlined in a speech today by John D. Podesta, the White House chief of staff. He said the policy tries to balance the privacy rights of computer users against the needs of law enforcement to be able to monitor digital communications.

Congress and federal regulators have done little work in the area, even as the world has quickly come to rely heavily on communications through cyberspace. More than 1.4 billion e-mail messages change hands every day.

The administration's legislative proposal on electronic surveillance tries to fix the inconsistent patchwork of laws that apply different standards to telephone, cable and other technologies with a single standard for those systems and the Internet. Prospects for the proposal in Congress are uncertain.

Until now, law enforcement agencies have been able to monitor electronic communication with only modest court supervision.

The proposed legislation would require that the same standards that apply to the interception of the content of telephone calls apply to the interception of e-mail messages. Specifically, it would require law enforcement agents to demonstrate that they have probable cause of a crime to obtain a court order seeking the contents of a suspect's e-mail messages.

The proposal would also give federal magistrates greater authority to review requests by law enforcement authorities for so-called pen registers — lists of the phone numbers called from a particular location and the time of the calls. The magistrates now have no authority to question the request for such lists, which are frequently used by the authorities.

In the context of the Internet, existing laws are ambiguous about what standards apply for different kinds of surveillance. Many limitations imposed on law enforcement in the context of telephone wiretaps — like the requirement that such taps be approved at the highest level of the Justice Department — do not appear to apply to e-mail surveillance.

Moreover, the Cable Act of 1984 sets a far harder burden for government agents to satisfy when trying to monitor computers using cable modems than when monitoring telephones. That has proved troublesome for law enforcement authorities as more Americans begin to use high-speed Internet service through cable networks. The Cable Act also requires that the target of the surveillance be given notice and an opportunity to challenge the request.

Concern that the proposals allow federal agents too much leeway.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Mr. Podesta said in a speech at the National Press Club. "Our proposed legislation would harmonize the legal standards that apply to law enforcement's access to e-mails, telephone calls and cable services."

White House officials said today that they hoped the proposal would break a logjam in Congress where a variety of different measures have been introduced dealing with electronic surveillance. The administration's proposal adopts some elements of both Democratic and Republican bills.

But Congressional aides said there was too little time left in the legislative session and that the matter would in all likelihood remain unresolved until after the next term begins, in 2001.

Administration officials said the proposal would apply to communications that either begin or end in the United States. It would not apply to e-mail messages transmitted entirely outside the country.

Privacy and civil liberties groups criticized the administration's proposal because it would continue to permit the government to use a new surveillance system that the groups say may be used far more broadly than older technologies, enabling federal agents to monitor an unlimited amount of innocent communications, including those of people who are not targets of criminal investigations.

The system, used by the Federal Bureau of Investigation, is called Carnivore, so named, agents say, because it is able to quickly get the "meat" in huge quantities of e-mail messages, so-called instant messaging and other communications between computers.

Carnivore is housed in a small black box and consists of hardware and software that trolls for information after being connected to the network of an Internet service provider. Once installed, it has the ability to monitor all of the e-mail on a network, from the list of what mail is sent to the actual content of the communications.

5/24/02 Release - Page 366

CONT'd

Doc # 5

Marcus C. Thomas, section chief of the Cyber Technology Section of the F.B.I., said the technology was developed 18 months ago by F.B.I. engineers and has been used fewer than 25 times. Mr. Thomas said that Carnivore had potentially broad capabilities and that he understood the concerns of privacy groups.

"It can do a ton of things," he said. "That's why it's illegal to do so without a clear order from the court."

He said that most Internet service providers had cooperated with requests to use Carnivore.

Privacy groups and some Internet service providers have been deeply critical of the use of Carnivore because, once installed on a network, it permits the government to take whatever information it wants.

Moreover, the government has not said what it does with the extraneous material it gathers that is not relevant to the particular surveillance.

The issue does not often arise today with the monitoring of telephone conversations because when a law enforcement authority wants to see a list of telephone calls made by a suspect, the agent gets an order from a magistrate, presents the order to a telephone company, and the company then turns over the list.

In at least one instance, an Internet company did not cooperate so readily with the government. In December, federal marshals approached the company with a court order permitting them to deploy a device to register time, date and source information involving e-mail messages sent to and from a specified account.

Trying to establish a single standard for different technologies.

Concerned the device would record broader information, the company countered with a compromise: it would provide the government with the requested information about e-mail senders and recipients, according to Robert Corn-Revere, a lawyer for the company, in recent Congressional testimony. The company was later identified as EarthLink, a service provider with 3.5 million subscribers.

Mr. Corn-Revere said the government initially accepted the compromise but later became dissatisfied and wished to use its own device. EarthLink objected but was overruled by a a federal court, which ordered the device deployed.

Other Internet companies have also been critical of Carnivore.

William L. Schrader, chairman and chief executive of PSINet, a major commercial Internet service provider, said that the system gave the F.B.I. the ability to monitor e-mail messages of every person on a given network. He said he would refuse to permit the government to use the technology at PSINet unless agents could prove that it could only sift out the traffic from a given individual that is the target of a court order.

"I object to American citizens and any citizens of the world always being subject to someone monitoring their e-mail," said Mr. Schrader, whose company serves about 100,000 businesses and more than 10 million users. "I believe it's unconstitutional and I'll wait for the Supreme Court to force me to do it."

Civil liberties groups, meanwhile, said that today's policy announcement was an inadequate response to the growing controversy over the deployment of Carnivore.

"Today's speech was camouflage to cover the mess that is Carnivore," said Barry Steinhardt, an associate director of the American Civil Liberties Union. "In light of the public and Congressional criticism of Carnivore, we had hoped and expected far more from an administration that likes to tout its sensitivity to privacy rights. Rather than glossing over Carnivore, Podesta should have announced that the administration was suspending its use."

Facing growing concerns about Carnivore, Attorney General Janet Reno said on Thursday that she would review whether the system was being used in a manner consistent with privacy rights in the Constitution and in federal law. A subcommittee of the House is set to hold a hearing next week on the system.

While the civil liberties and privacy groups applauded giving judges greater discretion to review certain kinds of requests for surveillance, they were critical of other aspects of the proposal.

Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology, criticized the administration for lowering the standards for surveillance of cable modems rather than raising the standards for telephone surveillance.

"The Cable Act provides for one of the best privacy protections in the United States," Mr. Rotenberg said. "The question is whether to harmonize up or harmonize down. Our view is this harmonizes down."

But administration officials said the Cable Act never contemplated that there would be broad use of cable modems for e-mail traffic and that the standards used for obtaining warrants for telephone surveillance should also apply to digital communications through cable networks.

2

The Washington Post

DATE: 2-18-00
PAGE: E-1

U.S. Hopes to Extend Online Wiretapping

By John Schwartz
Washington Post Staff Writer

The Clinton administration yesterday called for updating wiretapping laws to extend the powers of law enforcement to the online world while providing new legal protections for electronic communication.

Administration officials also announced, as expected, a plan to loosen controls on the export of encryption software—the programs that help Internet users scramble messages and data to protect them from prying eyes.

On the wiretapping issue, White House chief of staff John D. Podesta, in a speech at the National Press Club, described the coming legislative package as seeking to eliminate confusion about the level of legal protection for various forms of communication.

Telephone conversations get fairly strong protection from federal wiretaps under the 1968 Crime Patrol and Safe Streets Act, which required a court order and high-level Justice Department approval. Wiretape rules for e-mail sent by dial-up modem are covered by the Electronic Communications Privacy Act of 1986. That law might not cover e-mail sent by high-speed cable modem, and cable companies have argued that their online services should be given extremely high protection from government surveillance under the Cable Act.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Podesta said.

Lawmakers said they welcome the opportunity to work with the administration on these issues. Sen. Orrin G. Hatch (R-Utah), who has introduced an Internet privacy bill, said: "It is imperative that we balance the interests of law enforcement with the privacy rights of the American people. We must ensure that appropriate checks are in place where the government accesses private communications of Americans."

Podesta said the bills making up the package would be unveiled within 10 days, and that he hopes the legislation can be passed by the end of the year.

Podesta also spoke about the new surveillance technology known as Carnivore, which gives law enforcement authorities the ability to selectively monitor the Internet traffic of individuals, similar to the devices that can record the telephone numbers of calls made and received by a suspect. Unlike full-fledged wiretaps, the judicial oversight of such surveillance is slight, and the protection against abuses of the technology by law enforcement is weak. Podesta called for greater judicial oversight.

The Podesta speech was not well received by civil liberties advocates, who have fought Carnivore and other administration attempts to expand wiretapping capabilities on the Internet. Barry Steinhardt, associate director of the American Civil Liberties Union, called the speech "deeply disappointing. . . . While the Clinton administration's proposals have some heartening qualities to them, they are too little and too late," with too little time in the legislative session to pass new bills. The Carnivore system, Steinhardt said, "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic."

Podesta also discussed the new encryption policy, which the administration can implement immediately. Under the plan, U.S. companies will be able to export sophisticated cryptography products to users in any nation in the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The government will eliminate the statutory 30-day waiting period before such exports can take place but will keep in place a requirement that new technologies be submitted to the government for a technical review.

Encryption has been a high-tech battlefield from the early days of the Clinton administration. Few technologies are as important in the fight to maintain personal and business privacy, but few technologies present such daunting issues for law enforcement officials like FBI Director Louis J. Freeh, who often warns that criminals and terrorists can use "crypto" to cloak their plans and activities. High-tech companies successfully argued that U.S. restrictions harmed only American companies, since overseas firms were successfully marketing strong encryption products, and in January the Clinton administration reduced controls on encryption exports.

"The reducing of these regulations will certainly allow U.S. software makers to compete in the global marketplace," said Robert Holleyman, the chief executive of the Business Software Alliance.

3

DOC. #4

Los Angeles Times

DATE: 7-13-00
PAGE: A-8

Clinton Administration Seeks Updated Wiretapping Laws

From Associated Press

WASHINGTON—The White House proposed legislation Monday to update wiretapping rules so that legal protections currently applied to telephone calls are extended to electronic communication, such as e-mail.

The plan would require law enforcement officials to obtain high-level approval before applying for a court order to intercept the content of e-mail—in line with current rules that govern listening to phone calls.

"Basically, the same communication, if sent different ways—through a phone call or a dial-up modem—is subject to different and inconsistent privacy standards," said White House Chief of Staff John Podesta, in announcing the proposals. "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations."

The wiretap proposal also addresses so-called "trap and trace" orders, which allow law enforcement officials to identify the source of a phone call or an e-mail, but not its content. Under the proposal, law enforcement officials would only need one order—even to trace an e-mail or a phone call that may travel through multiple phone carriers or Internet providers.

Officials also could trace such communications without prior approval in an emergency situation, such as when a computer is under attack.

But for the first time, the administration is proposing that a federal or state judge independently determine whether the facts support such a trace order.

Officials were asked how those changes would impact the new "Carnivore" system, which the FBI is using to obtain e-mails of investigative subjects with a search warrant. When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

If the Carnivore system is being used to intercept the content of electronic communications, then law enforcement officials would need high-level Justice Department approval before obtaining a court order and stricter standards limiting its use would apply, Podesta said.

The FBI says the tool already is subject to intense oversight from its own internal controls, the Justice Department and the courts—with signification penalties for misuse of the system.

The proposed measures also would address inconsistencies in how current law applies to different networks carrying Internet traffic. For example, now that cable systems are being upgraded to offer two-way services, laws that apply to dial-up modems over phone lines should be extended to cable connections, Podesta said.

4

DOC # 7

THE WALL STREET JOURNAL

DATE: 7-18-00

PAGE: A3

Updating of Wiretap Law for E-Mail Age Is Urged by the Clinton Administration

By Ted Bridis
Staff Reporter of The Wall Street Journal

WASHINGTON—The White House is urging changes in U.S. law to make it easier for authorities to eavesdrop on Internet communications such as electronic mail, updating what the government described as wiretap laws written for an earlier era.

The administration said that the changes would enhance legal privacy protections because they would require, for example, approval by senior Justice Department officials before the Federal Bureau of Investigation could use software surveillance, such as its "Carnivore" system. That approval already is required in cases where law enforcement wants to monitor telephone conversations.

The changes require U.S. judges to suppress electronic evidence obtained by illegal wiretap; current law mandates suppression in such circumstances of only oral or written communications, not e-mail. The proposals were all made by the Justice Department in a March study that identified what the government said were deficiencies in enforcing laws against crimes on the Internet.

The American Civil Liberties Union said the White House announcement was "deeply disappointing," because it did not include any promise to suspend use of Carnivore, which the group charged gives the government "unsupervised access to a nearly unlimited amount of communications traffic."

The Internet Alliance, a Washington trade group for Internet providers, said the White House proposals "make sense," but also warned that its member companies "should not be deputized," a spokesman said.

The proposals were announced at the same time that the administration relaxed restrictions on the export of powerful encryption technology to the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. White House Chief of Staff John Podesta said the change, which will benefit some U.S. hardware and software firms, was not offered in exchange for the high-technology industry's support of the White House wiretap proposals. "We've never tried to link those two," he said.

The White House also sought to give authorities undisputed access to the Internet traffic of roughly 2.2 million consumers using cable modems. And it proposed making it easier for police to obtain court orders to trace the transmission and receipt of Internet data nationwide without asking permission from a judge in every jurisdiction the data passes through. Another change would give judges greater latitude in denying those requests. But in extraordinary cases, such as a hacker attack, the FBI could perform tracing, then obtain court approval as much as 48 hours later.

A legal dispute continues between Internet providers and law enforcement. The nation's cable Internet providers have argued that they are not required under the U.S. Cable Act to turn over subscriber information without giving customers the opportunity to fight the disclosure in court. However, the Justice Department argues it is entitled to cable Internet data under the Electronic Communications Privacy Act without warning the customer in advance about its proposed surveillance.

U.S. District Judge J. Young of Boston called the dispute "a thorny and important issue" in a case last year, in which he ordered an unidentified cable Internet provider to turn over the customer's records. Judge Young acknowledged that his decision should not be read too broadly, saying that it was "not the day to resolve such ephemeral puzzles."

Please Turn to Page A6, Column 3

Tapping Into Privacy

Some key changes the White House is seeking on Internet privacy:

- **Requiring higher level approval** by senior Justice officials to perform Internet wiretaps to read e-mail.
- **Requiring judges to discard** electronic evidence obtained in an illegal wiretap.
- **Mandating that Internet wiretaps** to read e-mail be used only when investigating the most serious crimes.
- **Requiring cable-Internet companies** to turn over customer information when presented with a judge's order.
- **Allowing authorities** to seek a single judge's order to trace Internet communications nationwide across different jurisdictions.

5

Doc. #8

Los Angeles Times

DATE: 7-18-00
PAGE: A-1

Restrictions Eased on Encryption Software Exports

By ASHLEY DUNN
and CHARLES PILLER
TIMES STAFF WRITERS

The Clinton administration on Monday further eased the remaining restrictions on selling high-powered encryption products overseas, clearing the way for American firms to export to the European Union and several other key trading partners.

The new policy drops a requirement that U.S. companies get a special license to sell encryption products—a process that previously involved a technical review or a 30-day delay.

In addition, the rules allow companies to sell their products to not only businesses and consumers, but also government agencies, which used to require a special license.

The rules apply to encryption exports to the 15 nations of the European Union, as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland.

The new rules follow the administration's major turnaround in January, when it finally opened the way for companies to export the hardest-to-crack scrambling technology.

American technology companies and privacy advocates had fought for years for permission to export its encryption technology abroad.

The industry argued that the spread of strong encryption would fuel electronic commerce and reassure consumers that their credit card numbers and other private communications would not be compromised.

White House Chief of Staff John Podesta, speaking at the National Press Club, described the changes announced on Monday as part of an ongoing effort to update U.S. policy.

"The Internet, like Morse's telegraph, brings with it new possibilities," he said. "It also brings new challenges to our most fundamental values and the need for new laws and new protections to maintain them."

Industry and security experts welcomed the latest announcement as another sign of the federal government's new-found support of liberalizing encryption exports.

"It's obviously very important if U.S. software companies are going to compete in the global market," said Amit Yoran a former Department of Defense security official and president of RipTech, a security company in Alexandria, Va.

According to Scott Schnell, senior vice president of RSA Data Security, a top encryption software producer, the new rules are important because they remove restrictions to selling to national governments.

Governments are often the biggest buyers of security software, particularly in the recently democratized nations of Eastern Europe.

"Both the relaxation and normalization around government use of the technology is a realization of the core importance of the security over the Internet," Schnell said. "This is a tremendous boost for the U.S. software industry."

But others said that until the regulations can be thoroughly reviewed by legal experts, their impact would be uncertain.

"The devil in this case is in the details," said Jeff Schiller, a leading security expert and network manager for Massachusetts Institute of Technology. Law enforcement and safety concerns remain, he said. "How are those addressed? I'd be very surprised if they were just lifting the controls."

He said that he suspects hidden restrictions could still bar the export of such products to the wrong countries.

"Let's say someone in one of the forbidden countries gets an account on America Online," Schiller said. "When they use their Web browser to get on the Net, it's going to say Virginia [where many AOL server computers that route Internet traffic are located]. I don't know they are from Libya. Under those circumstances who is responsible? Am I responsible? Is AOL responsible?"

But Schiller said that any relaxation of export controls is an acknowledgment of reality.

"You cannot turn the tide of technology back," he said. "The bad guys are going to do what they will do," while legitimate users of encryption products are harmed by export controls.

6

Doc #9

USA TODAY

DATE: 7-18-00
PAGE: 4-A

Rules on encryption exports are relaxed

The United States has eased its rules on exporting encryption products to the European Union and other key trading partners in an effort to improve security in cyberspace and promote electronic commerce, the White House said Monday.



By Dennis Cook, AP

Podesta: Change should not threaten U.S. security.

U.S. companies no longer need an export license to sell encryption products to users in the key trading countries, the White House said.

The policy allows U.S. exporters to ship their products without waiting for a technical review or a 30-day delay as they have in the past. Businesses and privacy advocates had said that U.S. export rules were too restrictive, but law enforcement officials said sophisticated encryption aids international criminal enterprises and terrorists. White House Chief of Staff John Podesta said the changes should provide adequate security.

The White House also proposed legislation to update wiretapping rules so that protections currently applied to telephone calls are extended to electronic communications such as e-mail. The changes could affect the system the FBI uses to access the e-mails of criminal suspects. Investigators would have to obtain high-level approval before seeking a court order.

7

Doc. # 10

The Washington Post

DATE: 7-16-02
PAGE: A-1

House Rejects Bill Limiting Web Gambling

Parties Sharply Divided; White House Opposed

By Dan Morgan
and John Schwartz
Washington Post Staff Writers

The House last night defeated a bill that would have banned most forms of online gambling, legislation intended to curb the explosive growth of casino-style wagering on the World Wide Web.

In a vote that reflected sharp divisions within both major parties over the issue, 44 Republicans joined 114 Democrats and one independent to defeat the measure. Under a procedure to bring the bill to the floor without amendments, a two-thirds vote of those present was required to pass the legislation. The final tally of 245 to 159 fell 25 votes short of the 270 needed.

The bill drew opposition from lawmakers and advocates concerned about federal regulation of Internet content, as well as the potential for invasion of privacy. Critics also raised concerns that to make the legislation palatable to the politically influential parimutuel horse racing and dog racing industries, GOP leaders had agreed to exemptions that would actually legalize an expansion of opportunities for online gambling.

The bill was intended to address growing fears among lawmakers about the explosive growth of unregulated online sites where individuals can engage in card games and other casino-style gambling on their computers. More than 700 such sites, many of them run out of foreign countries or offshore havens, are now operating without regulation, with roughly $1.2 billion wagered annually.

Under the bill defeated yesterday, state law enforcement agencies would have been able to go to court to obtain orders requiring Internet service providers to block access to Web sites that engaged in illegal gambling.

Before last night's vote, Rep. Robert W. Goodlatte (R-Va.), chief sponsor of the bill, cited a litany of social ills linked to gambling—crime, bankruptcy, addiction and more—and said that Internet gambling will bring citizens the same problems "as you would have if you had a casino in your home town."

But the White House said it "strongly" opposed the bill and stressed in particular its objections to the exemptions that would allow the parimutuel industry to conduct online betting under controlled conditions.

Although the Senate has passed a similar bill, it appeared unlikely last night that the GOP leadership in the House will attempt to bring the measure back to the House again this year given the limited time and the difficulty of crafting a compromise on such a complex issue.

Yesterday's vote was the culmination of one of the year's most hotly contested lobbying battles on Capitol Hill, generating a variety of strange alliances on both sides. Allied with the Las Vegas casino industry in support of the bill have been religious groups that are among the GOP's core group of supporters, including the Christian Coalition, the Southern Baptist Convention, the Family Research Council, and Focus on the Family.

But the booming high-tech industry, which the GOP is also courting, had serious concerns, and a number of governors objected that the legislation would not provide an exemption for state lotteries to sell tickets online within their own states.

Meanwhile, horse and dog racing venues have been fighting declining attendance, and stiffer competition from other forms of betting. They saw the bill as a way to ensure their long-term survival by allowing them to market their events over the Internet.

Goodlatte assured House members yesterday that the parimutuel provisions only authorized what is already legal under federal gambling law, and did not constitute an expansion. Action, he said, was essential on the larger issue of casino-type gambling.

But the White House charged that bill would have heightened the likelihood that children and other vulnerable groups would be able to get unsupervised, unlimited access to gambling activities on home computers.

"This bill appears to be designed to protect certain forms of Internet gambling that currently are illegal, while potentially opening the floodgates for other forms of illegal gambling," the White House said in a statement.

Along with concerns about the parimutuel betting provisions, some lawmakers in both parties expressed reservations about the extent of federal incursion into the prerogatives of the states.

"You would have the federal government dictate to Internet service providers what services they can offer," said Rep. Christopher Cox (R-Calif.) in opposing the legislation. He said it was "well-intentioned," but would "create enormous regulatory problems."

Goodlatte and the House GOP leadership sought to win more support for the bill with last-minute changes aimed at relieving some of the concerns of civil liberties groups. Rep. Jerrold Nadler (D-N.Y.) agreed to support the legislation only after language was added giving the operators of Web sites that have been shut down by court order up to 60 days to appeal.

Yesterday's outcome represented another in a series of sometimes awkward attempts by Congress to address the controversial issue of regulating Internet content. The Supreme Court struck down as unconstitutionally broad the 1996 Communications Decency Act, which made it a federal crime to make adult materials available to minors via computer.

Congress came back with the Child Online Protection Act, a narrower attempt to regulate commercial sites' showing pornography on the World Wide Web. That law has been challenged by civil liberties groups and publishers, and is currently before federal appellate courts.

THE WALL STREET JOURNAL

DATE: 7-19-00

PAGE: A-22

'Carnivore' Won't Devour Cyber-Privacy

By Bruce Berkowitz

On Monday the White House proposed new legislation regulating surveillance by law enforcement agencies on the Internet. But civil libertarians are already complaining that this plan does little to address the problems ostensibly raised by Carnivore, the FBI's new software system for performing court-ordered wiretaps at Internet service providers (ISPs).

Using a laptop computer, law enforcement officials can hook Carnivore into an ISP's network. Once installed, it reads the headers of each e-mail message—listing the sender, recipient and subject of the message—as it passes through. If the sender or recipient is the target of a tap, Carnivore records the message.

Rights at Risk?

Here's the rub: Before Carnivore can know whether a message belongs to a targeted party, it must browse the headers of all the messages passing through the ISP. With a traditional phone tap, law enforcement officers only listened to the telephone line that the subject of the tap was using. The ACLU and other critics complain that when Carnivore reads the headers of anyone who is not a target it violates their rights.

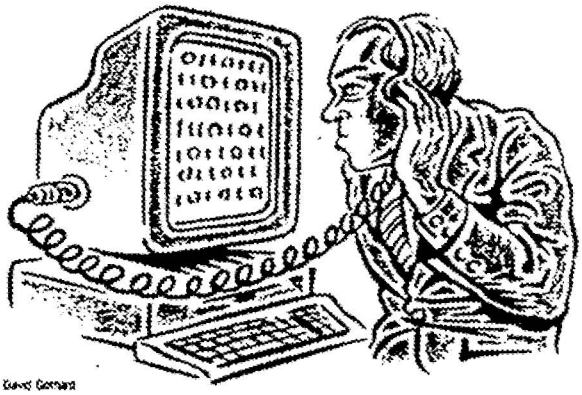
The ACLU and other Carnivore critics need to get a grip—and a better understanding of the new technology.

Unlike old-fashioned analog telephone calls, e-mail messages are transmitted digitally. A computer slices and dices the message into packets, each with an identifying tag. The packets then spread out throughout the Internet, finding the most efficient path to the destination. When they arrive, they are reassembled, and the recipient gets the message. As a result, with e-mail, you cannot "tap a line" because often there is, literally, no particular line to tap. All you can do is scan the messages that pass through a link a suspect is known to use—like his ISP—and pick out the ones that belong to him. That's what Carnivore does.

The ACLU complains that using a computer to monitor an ISP system would collect vast amounts of innocent data. But what do they expect the feds to use—a typewriter and an abacus? Note to FBI: Hire a better public relations firm, and name your next project "Vegetarian."

These kinds of flaps are happening more and more often. Last April some privacy advocates complained when the FBI requested $15 million for "Digital Storm," a program for monitoring telephone calls and analyzing recordings. In September, a programmer in North Carolina found the notation "NSA Key" in a Microsoft software patch. Soon rumors bounced through the Internet claiming Windows had a back door that allows the National Security Agency to monitor your computer. (Microsoft explained that the tag merely signified that the software complied with the agency's security standards.)

There's a lot of concern about the ability of governments to monitor communications in the digital age. In fact, it's getting harder, not easier, for them to listen in.



The granddaddy of all bogus fears, though, is Echelon. If you believe some European Union parliamentarians, the United States and Britain operate an international network that monitors virtually all communications, and extracts choice nuggets with powerful computers that recognize key phrases in messages like "assassination," "terrorist attack" or "industrial secret."

In reality, it's not easy to find a specific message in a flood of free-flowing digital data. That's the whole reason for getting a court order for a wire tap. If you cannot hook into an ISP, you have to do a lot of searching to find the message you want to intercept.

That is also why the European campaign against Echelon is so quixotic. True, the folks at NSA intercept communications and they have powerful computers and ingenious software that helps with the processing. But it is impossible for even the best computer system to routinely sort through all of the world's telecommunications and pull out telltale messages, as the Echelon paranoids would have you believe.

Usually you need to know what you are looking for and where the message might appear before you have much of a chance of finding it. Also, the cases in which one message tells a whole story are rare. Good law enforcement and intelligence usually requires multiple sources and collateral information to make sense of an intercept.

The privacy advocates have the story reversed. It's getting harder, not easier, for our law enforcement and intelligence organizations to listen in on communications. In the old days you could tap a line or intercept a microwave link. It's much more difficult to capture digital messages that pass over fiber optics or bounce through cellular networks. And, with strong encryption software freely available world-wide, anyone really determined to keep a message secret can usually do so.

If you have any doubts, just recall how many intelligence surprises we have had lately—the Indian nuclear test, the North Korean missile test, the terrorist bombings of American targets in the Mideast and Africa. Part of the problem is that we cannot get to many of the sources that we used to, and everyone is getting better at concealing their communications.

57

cont'd

So why is it so easy to stir up these controversies about privacy? The simple fact is that relations between the government and the new information industries are lousy. There is too much suspicion and too little communication.

The administration gets part of the blame for its ham-handed policies. Carnivore is a good example. A lot of controversy could have been defused if the FBI had offered more insight into how the system worked and how the rights of non-suspects would be protected.

But the record of the technogeeks has not been much better. They often act as though law enforcement officials have no business poking into their activities at all—as though one could stop international computer criminals with a good neighborhood watch program.

It's all too easy to lose sight of the fact that Carnivore's main targets are cybercriminals—in other words, the kinds of crooks who are a plague on the Internet and target dot-com companies. Growth rates for Internet shopping have been slipping lately. According to some experts, people worry about whether their credit card numbers and health records are safe. You would think that e-business would be the first to support better law enforcement on the net.

Common Goals

All the good guys in this dispute have common goals. Defense and intelligence officials want to protect the nation's communications infrastructure. Law enforcement officials want to chase crooks, and companies want the cops to catch them. Consumers want privacy. The path to all is the same: secure information systems, reasonable cooperation from the private sector, and aggressive law enforcement and effective intelligence closely monitored by responsible public officials.

Fixing the relationship between Washington and Silicon Valley needs to be a top priority for the next administration. The only people benefitting from controversies like the one over Carnivore are terrorists, criminals and rogue states.

Mr. Berkowitz is a research fellow at the Hoover Institution and coauthor of "Best Truth: Intelligence in the Information Age" (Yale University Press, 2000).

58

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #8, OGC FRONT OFFICE FILE (Pgs 849

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #13 (Pages 376-377)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Questions for the Record
June 20, 2000

Senator Kyl:

Q: Is the NIPC able to provide indications and warnings of an attack? For example, does the Center have the ability to detect anomalous activity or patterns in key communications nodes that might indicate something is about to happen?

The NIPC's ability to perform "indications and warning" is dependent first and foremost on its ability to quickly gather information from multiple sources about an ongoing or imminent attack (whether an intrusion, a virus, a denial of service, or other form of attack). The NIPC does not operate any detection mechanisms on any government or civilian systems. Thus, we do not get "indications" in an automated sense from any detection devices. In this sense, I&W in the cyber world is very different from I&W in the nuclear missile or conventional weapons world, where radars and other devices can provide advanced warning of an attack. Rather, we get relevant information from intelligence sources, criminal investigations, "open sources" (such as media and the Internet), and from industry and government contacts. We "detect" anomalous activity in key communications nodes only if the owner/operator of that node detects it and informs the NIPC, an FBI Field Office, or another agency, or if we learn through criminal investigation or intelligence sources that the node is being attacked. The key to the NIPC's ability to do this is the development of connectivity and close interaction with numerous Defense and Intelligence Watch centers, FBI Field Offices, other Law Enforcement organizations, computer anti-virus association groups, private and public Computer Incident Response Teams (CIRTs) and Computer Emergency Response Teams (CERTs), foreign law enforcement agencies, and private industry (both individual companies and information sharing organizations). Over the past two years, the NIPC has made substantial progress in developing these relationships, but this is a continuing task and more work remains to be done. One of the main reasons for our extensive outreach programs is to build trust and willingness on the part of private companies to report cyber incidents to us, and these efforts are bearing fruit. In addition, PDD-63 directs other federal agencies to report incidents to the NIPC directly. Many agencies are doing this, but there is room for improvement with others. In addition to reports from companies and agencies, the NIPC Watch actively scans all available governmental and private sector sources for reports or information regarding cyber activity, and interacts throughout each day with other watch centers to share information.

Once information (or "indications") of an attack is received and analyzed, the NIPC can issue a warning, alert, or advisory through numerous means, depending on the appropriate audience. Warnings can be issued to specific targeted companies through FBI Field Offices or by the watch directly; other federal agencies can be notified by e-mail, secure facsimile, and telex; state and local law enforcement can be warned by NLETS; industry can be warned through InfraGard secure email and website and through ANSIR (an e-mail system that reaches tens of thousands of companies); and the general pubic can be warned via the NIPC webpage and the

5/24/02 Release - Page 178

Doc. #14

news media. All of these mechanisms have been used numerous times (as discussed in the answer to the next question).

Senator Kyl's question goes to the heart of I&W in the cyber world: should the Nation have the capability to detect intrusions into government or private sector systems in an automated fashion, without having to rely on human detection and reporting? The controversy attending the Administration's recent "FIDNET" initiative, which is a limited proposal to place automated intrusion detection devices on federal agency networks, identified many of the privacy and other issues such a system would raise, particularly if it were extended to privately owned networks. The government's approach at the present time is to encourage industry to protect and monitor its own systems, and to report anomalous activity voluntarily. The NIPC works within that overall policy to encourage private sector reporting as a critical part of its I&W. Examples of this include InfraGard and the incident reporting pilot program we have developed with the energy sector through the North American Electrical Reliability Council (NERC).

Q: How many warnings has the NIPC issued which were developed through the Centers's own analysis of activity?

Of the 54 tactical warning products disseminated since the NIPC was established in February 1998, all were developed in whole or in part through the Center's organic analytical capability and analysis of activity. Some of these products were initiated by the NIPC (e.g., the BAT/Firkin Worm, also known as the "911" Worm), while others built upon basic analysis initiated elsewhere (e.g., the NIPC assessments of Distributed Denial of Service tools). We cannot put a precise figure on the relative contributions, since these are all community-collaborative products. In performing analyses and issuing warnings, the NIPC works closely with other government agencies, private sector organizations such as CERT (which is an FBI contractor), and the SANS institute, and academic institutions.

In addition to warning products, the Center has produced hundreds of non-warning informational products. Since 1998 the NIPC has produced 301 daily reports, 30 CyberNotes (a summary and analysis of technical exploits and vulnerabilities), 51 Critical Infrastructure Developments reports (a report on recent cyber-related issues and incidents), and five IP Digests (a periodic, in-depth analysis of cyber threats and vulnerabilities). Versions of these analytical products go to private industry, to the Intelligence Community, other federal agencies (including law enforcement), and to criminal investigators.

Q: What other agencies do you see playing a significant role in the area of computer crime investigations?

Cyber crime is an issue that concerns not just the FBI, and not just law enforcement generally. Indeed, "cyber crime" in itself should be seen as part of a broader array of cyber threats, including cyber terrorism, cyber espionage, and information warfare, since all are closely related and often difficult to distinguish at the outset of an incident. As a result, cyber threats are

of great concern to numerous federal agencies, including the Defense, Intelligence, and Law Enforcement Communities and to civilian "Lead Agencies" under PDD-63; to state and local governments, including law enforcement; and, of course, to the private sector. It is because of this wide-ranging interest that the NIPC was established as an interagency center. The NIPC provides a locus and mechanism for coordinating the expertise and roles of many agencies, and facilitates information sharing and operational coordination. The NIPC works closely on investigative matters with many law enforcement agencies, including: the Secret Service, Internal Revenue Service (IRS), Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), United States Air Force Office of Special Investigations (AFOSI), Defense Criminal Investigative Service (DCIS), National Aeronautics and Space Administration Office of Inspector General (NASA OIG), Department of Energy (DOE), state and local law enforcement, the Intelligence Community, as well as foreign law enforcement agencies through FBI Legal Attaches (LEGATS).

Q: Are there reasons, other than funding, which have caused other agencies to pull their personnel out of the NIPC? For example does FBI management at the Center recognize the expertise of the other agencies and allow them to fully participate?

One of the difficulties in attempting to operate an interagency Center is ensuring that all relevant agencies participate. Agencies have not received direct funding to participate in the Center, and so must take detailees to the NIPC out of existing personnel resources. In addition, personnel with cyber expertise are unfortunately in very short supply, meaning that agencies must commit to take scarce resources and send them outside their agencies. Despite these impediments, numerous agencies have sent detailees to the NIPC, including: Defense/Office of the Secretary of Defense; Central Intelligence Agency; National Security Agency; Air Force Office of Special Investigations; U.S. Navy; U.S. Army; U.S. Postal Service; Defense Criminal Investigative Service; General Services Administration; U.S. Air Intelligence Agency; Department of Commerce, and the Tuscaloosa, AL Sheriff's office. In addition, we have foreign liaison representatives from two allied countries who assist in coordinating international activities with our counterparts. A representative from FAA is also scheduled to start at the end of June. Additional representative from DoD, CIA, and NSA are also slated to arrive in the near future. We are also expecting representatives from local Washington area police departments on a part-time basis.

Some agencies were represented earlier but do not currently have representatives. Circumstances necessitated the recall of the first State Department representative. State agreed to do so, and has committed to NIPC that it would replace him with two new representatives. DoE's first representative rotated back after more than two years. NIPC's understanding as to why this representative rotated back is that he was at NIPC for a lengthy time and was needed at DoE headquarters to assist in a DOE reorganization. DoE has committed to replacing that detailee.

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has

5/24/02 Release - Page 380

not yet committed to replacing them. Secret Service has not provided any written explanation for this, but in oral discussions, Secret Service officials stated that USSS was not getting additional funding for its electronic crimes program despite its participation in NIPC; the FBI was receiving more media attention in the cyber crime area; and NIPC had not "referred" cases to Secret Service for investigation. NIPC offered any support it could give to Secret Service in addressing budget requests; noted that NIPC public statements often referred to partnership with USSS; and offered to do more to support USSS initiatives with public statements and case analyses. NIPC also stated (as discussed further below) that its role is not to create and "refer" cases; rather, cases generally originate in Field Offices, and FBI and Secret Service field offices frequently work computer crime cases together.

NIPC fully recognizes the value other agencies bring to the cyber crime and infrastructure protection mission. That is why NIPC is an interagency Center, and has senior managers from other agencies in addition to investigators and analysts. For instance, the NIPC Deputy Director is from DoD/OSD; the Section Chief of the Analysis and Warning Section is from CIA; the Assistant Section Chief of the Computer Investigations and Operations Section is from Air Force OSI; the Unit Chief of the Analysis and Information Sharing Unit is from NSA; and the Unit Chief of the Watch and Warning Unit is from the U.S. Navy. Secret Service formally occupied the position of Assistant Section Chief of the Training, Outreach, and Strategy Section. Recognition of the need for other agency participation is also what drives NIPC to continually seek additional representatives from other agencies. It is also reflected in the numerous joint investigations that NIPC and FBI Field Offices have been involved in with other agencies (as discussed further below).

Q: How many criminal investigations have been referred from the NIPC to these other agencies? Does the Center have operating procedures to refer a case to another agency?

As a general matter, the NIPC does not "refer" cases. Cases are normally initiated by a field office, whether a Field Office of the FBI, the Secret Service, another federal agency, or a state or local law enforcement agency. NIPC is the "program manager" of the FBI's computer intrusion investigative program, and so receives information about cases directly from the FBI Field Offices. Under PDD 63, other agencies are also supposed to report information about cyber incidents to the NIPC. Sometimes, NIPC will receive the first report of a cyber incident from a private company, a government agency, or another source, and contact the appropriate FBI Field Office. If another agency has concurrent investigative jurisdiction or some other non-investigative interest, that agency will also be contacted (either by the FBI Field Office of the NIPC). Where joint jurisdiction exists, the FBI field office may work jointly with the relevant other agencies (as discussed further below).

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations

under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

There have been, however, several instances in which the NIPC or an FBI field office has contacted another agency to determine if that agency wanted to conduct an investigation either jointly or separately, but that agency declined. A couple of examples are listed below.

In May 2000, the FBI's Detroit Field Office referred a complaint to the local Secret Service office regarding a denial of service attack against NHL.com, going so far as to transfer the call from the FBI field office to the Secret Service field office. The Secret Service told the complainant that no one was in the office to receive the complaint due to a visit of Texas Governor George W. Bush to Michigan. The complainant then called the FBI again and the Detroit Field Office took the complaint and assigned the matter for investigation.

Also in May 2000, based on FBI source information, the NIPC notified the USSS headquarters that there may be a vulnerability with the White House Webpage that gave the public access to all the files on that server. The USSS advised that the system administrator may already be aware of this. Neither the NIPC nor the FBI's Washington Field Office has heard back from the USSS regarding this matter.

In another instance, the FBI's Williamsport, Resident Agency, part of the Philadelphia Field Office, opened an investigation into a series of computer intrusion into 10 companies resulting in the loss of approximately 28,000 credit card numbers. During the initial investigation, the FBI discovered that one of the victims located in Buffalo, NY, had contacted the Secret Service and the USSS had opened a case pertaining to the intrusion against the single victim company, but was not investigating the larger set of thefts. The FBI contacted the Secret Service Division in Buffalo, NY to coordinate the case, since USSS already had a pending investigation. The FBI was told that due to the Security Detail Duties for the First Lady, the USSS would be unable to coordinate at the present time with the FBI on the case.

Q: In previous testimony before this subcommittee Mr. Vatis has stated that the NIPC has referred approximately 800 cases for criminal investigation. How many of these 800 cases actually involved a real threat to our nation's critical infrastructure? Would you catagorize the recent Denial of Service attacks launched last month as an attack on our nation's critical infrastructure?

In previous testimony before the subcommittee, the approximate 800 number of cases that Mr. Vatis referenced were not cases the NIPC "referred," but was the number of computer intrusion, denial of service, or virus cases pending in FBI field offices at the time of testimony. As of May 1, 2000 there were 1,072 pending investigative cases.

5/24/02 Release - Page 382

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus of these 1,072 cases, there is no methodology to determine which ultimately constitute a threat to our nation's critical infrastructure. However, we can cite several examples.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

Q: Besides Solar Sunrise and Moonlight Maze, what other joint investigations can you point to that demonstrate successful interagency cooperation?

Since the founding of the NIPC in February 1998, there are numerous cases which have demonstrated successful interagency cooperation other than the significant Solar Sunrise and Moonlight Maze cases. The importance of these two cases should not be overlooked, however. Both represent significant milestones in building awareness of the cyber threat among federal agencies and policymakers, demonstrated significant vulnerabilities in DoD and other government systems, and provided opportunities to test and improve the NIPC's processes for interagency coordination.

5/24/02 Release - Page 383

The following cases represent a small sample of these cases which have been successfully worked with other agencies:

DDOS: Numerous Internet commerce sites have been victimized by DDOS attacks since February 7, 2000. These DDOS attacks prevented the victims from offering their web services on the Internet to legitimate users. A DDOS attack uses compromised computer networks to "flood" a victim's computer network with massive amounts of data, which causes the victim's computer network to become overwhelmed and to stop operating. The DDOS attack investigation are investigations in seven FBI field offices, five overseas Legal Attache offices, other government agencies such as NASA, as well as the Royal Canadian Mounted Police. Reflecting the extraordinary level of cooperation on these investigations, on April 15, 2000, the Canadian officials arrested a juvenile charging him with one of the attacks.

Curador: On March 1, 2000, a computer hacker using the name, "Curador", allegedly compromised multiple E-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers. Thousands of credit card numbers and expiration dates were posted to various Internet websites. On March 9, 2000, InternetNews reported that Curador stated, "Law enforcement couldn't hack their way out of a wet paper bag. They're people who get paid to do nothing. They never actually catch anybody." After an extensive international investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (UK) Police Service in a search at the residence of Curador; Curador, age 18, was arrested in the UK, along with an apparent co-conspirator under the Computer Misuse Act 1990. Under United Kingdom law, both males have been dealt with as adults. Loss estimates are still being determined.

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Burns: In August 1998, the FBI initiated an investigation on an individual only known as "zyklon," who conducted numerous computer intrusions to various computer systems causing damages to websites and system files. The case was worked in cooperation with the Virginia State Police. The investigation identified zyklon to be Eric Burns of Shoreline, Washington. In February 1999, following an execution of a search warrant, Burns confessed to the intrusions. In May 1999, Burns also gained unauthorized access and defaced the webpage for the White House website. At that point the FBI began working with the U.S. Secret Service on the case. In September 1999, Burns pleaded guilty to one count for violation of Title 18 USC Section 1030 (Computer Fraud and Abuse) for one of the 1998 intrusions. In the plea agreement, Burns also admitted his criminal activity into several other intrusions including the White House website. In November 1999, Burns was sentenced to 15 months in prison, 3 years supervised release and $36,240 in restitution and a $100 fine.

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

Mewhiney: Throughout 1996, National Oceanic and Atmospheric Administration (NOAA) suffered several computer intrusions which were also linked to intrusions occurring a the National Aeronautics and Space Administration (NASA). These computer intrusions continued through 1997. The FBI worked the case jointly with NOAA, NASA, and the Canadian authorities and identified the subject, Jason G. Mewhiney, who resided in Canada. The original damage assessment that Mewhiney had caused, exceeded $40,000. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, Mewhiney pleaded guilty to 12 counts of intrusions which included violations spanning from May 1996 through April 1997, of destroyed/altered data and intrusions with the intent to damage. In the Canadian Superior Court of Justice, Mewhiney was sentenced to 6 months in jail for each of the counts to run concurrently.

Bliss: In February, 1998, the FBI opened an investigation to assist the U.S. Air Force and U.S. Navy regarding multiple computer intrusions. The case was worked jointly with the U.S. Naval Criminal Investigative Service and Florida State Attorney's Office in Jacksonville, FL. The subject was identified as Jesse Le Bliss, a student of the University of North Florida. On August 21, 1998, Bliss pleaded guilty to one felony count for violation of Florida State Statute 815.06 entitled, Offenses Against Computer Users. On September 19, 1998, Bliss was sentenced in the Fourth Judicial Circuit, State of Florida, to six months house arrest followed by three years probation, 200 hours of community service, and a written letter of apology to the Commandant of the United States Marine Corps.

CD Universe: One pending case being worked by the FBI's New Haven Division and the U.S. Secret Service has been widely reported in the press, due to statements made to reporters by the alleged perpetrator. In December 1999, the FBI's New Haven Division opened a case into the intrusions into the computers of CD Universe, an on-line music seller, and the theft of customers' credit card numbers and a related extortion attempt. Because of the credit card aspect, the FBI called the USSS to ask if USSS wanted to investigate jointly. The USSS declined. In January

2000, the New York Times ran a front page story about the case, based on conversations between the reporter and the alleged perpetrator. Subsequently, USSS called the FBI back and requested to work the case jointly. That case is still pending.

Other

There are other investigations that are being conducted with other agencies, however further details may adversely impact the investigation due to their pending status. There are currently 47 pending investigative cases which are being worked jointly between the FBI and the multiple entities of the Department of Defense. An additional 58 cases were investigated jointly with other entities that are now in closed status.

5/24/02 Release - Page 386

Senator Feinstein:

1. Under Presidential Decision Directive 63 (PDD 63), the ..[sic... NIPC]... is supposed to take the lead in warning of, investigating, and responding to threats to or attacks on this country's critical infrastructures. NIPC includes representatives from the FBI and other law enforcement agencies. You testified that the NIPC has improved the FBI's ability to fight cybercrime and that the FBI closed 912 cybercrime cases in the Fiscal Year 1999 and had 834 pending cybercrime cases that year.

How many of the 912 closed cases involved threats to or attacks on our nations's critical infrastructures? Were these cases really a threat to our national security? What about the pending cases? How many involved threats to or attacks on our nation's critical infrastructures?

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus, there is no methodology to determine which cases ultimately constitute a threat to our nation's critical infrastructure.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on

5/24/02 Release - Page 387

the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

2. In testimony last February 16, you said that the FBI was producing "fast-developing leads" and that a break in the case was imminent. A couple of weeks later, Michael Vatis, director of NIPC, suggested that in fact agents were making slow progress in the case.

How would you assess progress in the case now?

In fact, the testimonies of FBI Director Freeh and NIPC Director Vatis were entirely consistent. Both cited the difficulties in conducting cyber crime investigations, but both also expressed optimism about the prospects for a successful resolution of the case. Director Freeh's February 16 testimony for the record contained the following remarks about the DDOS investigation:

> On February 8, 2000, the FBI received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship the NIPC has developed with the private sector, in the days that followed, several other companies also reported denial of service outages. These companies cooperated with our National Infrastructure Protection and Computer Intrusion squads in the FBI field offices and provided critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages.
>
> *The resources required in these investigations can be substantial.* Already we have five FBI field offices with cases opened: Los Angeles, San Francisco, Atlanta, Boston, and Seattle. Each of these offices has victim companies in its jurisdiction. In addition, so far seven field offices are supporting the five offices that have opened investigations. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers, and providing all-source analytical assistance to field offices. Agents from these offices are following up literally hundreds of leads. While the crime may be high tech, investigating it involves a substantial amount of traditional police work as well as technical work. For example, in addition to following up leads, NIPC personnel need to review an overwhelming amount of log information received from the victims. Much of this analysis needs to be done manually. Analysts and agents conducting this analysis have been drawn off other case work. In the coming years we expect our case load to substantially increase. (Emphases added.)

NIPC Director Vatis' February 29 testimony for the record contained the following statement about the DDOS investigation:

5/24/02 Release - Page 388

On February 8, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

The resources required in an investigation of this type are substantial. Companies have been victimized or used as "hop sites" in numerous places across the country, meaning that we must deploy special agents nationwide to work leads. We currently have seven FBI field offices with cases opened and all the remaining offices are supporting the offices that have opened cases. Agents from these offices are following up literally hundreds of leads. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers (ISPs), and providing all-source analytical assistance to field offices. Moreover, parts of the evidentiary trail have led overseas, requiring us to work with our foreign counterparts in several countries through our Legal Attaches (LEGATs) in U.S. embassies.

While the crime may be high tech, investigating it involves a substantial amount of traditional investigative work as well as highly technical work. Interviews of network operators and confidential sources can provide very useful information, which leads to still more interviews and leads to follow-up. And victim sites and ISPs provide an enormous amount of log information that needs to be processed and analyzed by human analysts.

Despite these challenges, I am optimistic that the hard work of our agents, analysts, and computer scientists; the excellent cooperation and collaboration we have with private industry and universities; and the teamwork we are engaged in with foreign partners will in the end prove successful. (Emphases added.)

Indeed, the FBI's investigation, conducted in close coordination with the Royal Canadian Mounted Police, very quickly had resulted in the identification of one subject in Canada. Because additional evidence needed to be gathered by the RCMP in the DDOS case and in another matter that came to light during the RCMP's investigation, the subject could not be immediately arrested, and the investigation's progress could not be discussed publicly. However, on April 15, the RCMP executed a search warrant and arrested a juvenile charging him with one of the attacks.

5/24/02 Release - Page 389

We would therefore assess the progress in this case as substantial and, indeed, unprecedented in a case of this scope and nature. The investigation continues into the attacks on DDOS victims, and we believe good progress continues to be made.

3. In testimony last February 16, you suggested that the FBI's resources "are stretched paper-thin" because of the lack of high-caliber government forensic computer experts.

How much has this contributed to the government's lack of success in catching the perpetrators of the February cyber attacks?

As discussed above, substantial progress in fact has been made in the DDOS investigation, with one subject already identified in Canada.

That said, given the explosive growth in computer crimes, our existing resources both in the Computer Analysis Response Team and in the NIPC and the related field office National Infrastructure Protection and Computer Intrusion Program are indeed stretched paper thin.

The Laboratory Division's CART team supports the investigation of any sort of criminal investigation in which evidence might be found on a computer (such as a drug trafficker's accounts) by conducting computer forensic examinations on seized media. The Lab's technically trained agents develop, deploy, and support equipment to perform Title III and FISA interceptions of data communications on the Internet. Staff in both of these areas (forensics and engineering support) is extremely stretched because these agents are tasked with providing support not only for cyber crimes, but all traditional crimes in which digital evidence may be present or data interception required.

The FBI's CART program, consisting of agents and analysts who examine digital medial in order to gather evidence, is not able to keep up with the increasing workload. The following is a summary of current and future trends assuming that the FBI Laboratory is funded for all pending budget requests:

CART Capacity and Backlog

Year	FTE Staffing	Capacity	Exam Requests	Case Backlog	Backlog Time (Months)
1999	95	1900	3500	1600	10.1
2000	104	2080	5000	2920	16.8
2001	154	3080	6000	2920	11.4
2002	213	4260	8500	4240	11.9

5/24/02 Release - Page 390

In addition, the FBI's Laboratory Division currently provides support not only for FBI cases, but also for the Drug Enforcement Administration and the Immigration and Naturalization Service.

The NIPC and the field office NIPCIP squads are responsible for conducting investigations of cyber attacks, including computer intrusions, viruses, and denials of service. The NIPC currently has 193 FBI Special Agents in the field offices investigating approximately 1200 computer intrusion and other "NIPCIP" cases. Only 16 Field Offices have full squads of seven or more agents. The other field offices have only 1 to 5 agents, who are responsible for not only cyber investigations, but also for industry liaison, the InfraGard Initiative, the Key Asset Initiative, and support to other investigative programs. Further, the NIPC lacks sufficient computer scientists and analysts to support the field office investigations. For instance, it has only 7 network analysts/electrical engineers to support investigations such as DDOS attacks.

The NIPC's and Field Office resources have remained relatively static. The NIPC Headquarters budget for fiscal years 99-01 has been as follows:

Fiscal Year	Budget Authority
1999	29,057,000 (included one-year funding of $10 million for special contingencies in Attorney General's Counter-terrorism Fund)
2000	19,855,000
2001 requested	20,396,000

Meanwhile, our pending case load has grown rapidly.

Fiscal Year	Pending Case Load at end of fiscal year
1998	601
1999	801
2000 (as of May 1)	1072

Clearly, then, resources have not kept pace with the crime problem.

Evidence gathering for computer intrusions mandates a prompt response because the digital evidence trail can disappear so quickly. The complexity of documenting, examining and analyzing the tremendous amount of information that is necessarily collected in these types of cases and its very technical nature requires investigators, examiners, and analysts with extremely

5/24/02 Release - Page 291

specific skills and experience. Because of the technical nature of this crime, it is difficult, if not impossible, to temporarily assign additional Special Agents to an investigation since a special technical skill set is required to investigate such matters.

Staff shortages impede not only our ability to conduct investigations adequately, but also to quickly obtain information, conduct analyses, and craft and issue appropriate warnings and alerts. This makes the Indications and Warning mission much more difficult to perform.

4. Some have argued that the high-profile February attacks on Yahoo, eBay, and other companies were just a diversion, allowing the hackers to focus on making smaller, intrusive attacks on smaller sites.

Have you found any evidence for this contention?

No. There are individuals and groups who do focus on planning and executing more intrusive attacks, often for the sake of stealing information or money, but we have not seen any correlation between such intrusions and the February DDOS attacks.

5. Why don't you think industry can solve this problem itself?

The Internet was not designed with security as the foremost consideration. Moreover, until very recently, security was not a major priority of either hardware/software manufacturers or consumers. As a result, networks are still rife with vulnerabilities. Improving security on the Internet is thus first and foremost the responsibility of industry. Government must protect its own systems, and can assist industry by providing information about threats and vulnerabilities that we are aware of, and the NIPC does that. But it is industry's responsibility to secure privately owned systems.

Even if systems were more secure, however, there would inevitably be some amount of computer crime committed on the Internet – including not just intrusions, denials of service, and viruses, but also traditional crimes perpetrated over the Internet such as fraud and dissemination of child pornography. As long as crime exists, the public will expect law enforcement to investigate and apprehend the perpetrators. And effective law enforcement is a key element in any strategy to deter further criminal activity. Thus, industry and law enforcement must work closely together.

6a. How big a problem is this for the FBI? Do you believe that there are important cyber attacks that are never investigated by law enforcement because the attacked companies refuse to report them?

The vulnerabilities that permeate the industry are a big problem for the FBI and other law enforcement agencies because they make it so easy for crimes to be committed. This accounts in

5/24/02 Release - Page 392

Senator Grassley

1. Of the 800 cases referred for criminal investigation in FY 1999 from the NIPC, what percentage of these cases were referred to other agencies, other than the FBI, for continued investigation and possible criminal prosecution?

As a general matter, the NIPC does not "refer" cases. Cases are normally initiated by a field office, whether a Field Office of the FBI, the Secret Service, another federal agency, or a state or local law enforcement agency. NIPC is the "program manager" of the FBI's computer intrusion investigative program, and so receives information about cases directly from the FBI Field Offices. Under PDD 63, other agencies are also supposed to report information about cyber incidents to the NIPC. Sometimes, NIPC will receive the first report of a cyber incident from a private company, a government agency, or another source, and contact the appropriate FBI Field Office. If another agency has concurrent investigative jurisdiction or some other non-investigative interest, that agency will also be contacted (either by the FBI Field Office of the NIPC). Where joint jurisdiction exists, the FBI field office may work jointly with the relevant other agencies (as discussed further below).

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

There have been, however, several instances in which the NIPC or an FBI field office has contacted another agency to determine if that agency wanted to conduct an investigation either jointly or separately, but that agency declined. A couple of examples are listed below.

In May 2000, the FBI's Detroit Field Office referred a complaint to the local Secret Service office regarding a denial of service attack against NHL.com, going so far as to transfer the call from the FBI field office to the Secret Service field office. The Secret Service told the complainant that no one was in the office to receive the complaint due to a visit of Texas Governor George W. Bush to Michigan. The complainant then called the FBI again and the Detroit Field Office took the complaint and assigned the matter for investigation.

Also in May 2000, based on FBI source information, the NIPC notified the USSS headquarters that there may be a vulnerability with the White House Webpage that gave the public access to all the files on that server. The USSS advised that the system administrator may already be aware of this. Neither the NIPC nor the FBI's Washington Field Office has heard back from the USSS regarding this matter.

In another instance, the FBI's Williamsport, Resident Agency, part of the Philadelphia Field Office, opened an investigation into a series of computer intrusion into 10 companies resulting in the loss of approximately 28,000 credit card numbers. During the initial investigation, the FBI discovered that one of the victims located in Buffalo, NY, had contacted the Secret Service and the USSS had opened a case pertaining to the intrusion against the single victim company, but was not investigating the larger set of thefts. The FBI contacted the Secret Service Division in Buffalo, NY to coordinate the case, since USSS already had a pending investigation. The FBI was told that due to the Security Detail Duties for the First Lady, the USSS would be unable to coordinate at the present time with the FBI on the case.

In addition, the FBI has worked, and continues to work, many investigations jointly with other agencies. Two notable examples include Solar Sunrise and Moonlight Maze. Both cases involved extensive intrusions into Department of Defense and other government agency computer networks. The investigations involved an NIPC-coordinated investigation involving numerous law enforcement, intelligence, and defense agencies, as well as foreign law enforcement agencies.

Beyond those examples, the following are other instances of joint investigations.

DDOS: Numerous Internet commerce sites have been victimized by DDOS attacks since February 7, 2000. These DDOS attacks prevented the victims from offering their web services on the Internet to legitimate users. A DDOS attack uses compromised computer networks to "flood" a victim's computer network with massive amounts of data, which causes the victim's computer network to become overwhelmed and to stop operating. The DDOS attack investigation are investigations in seven FBI field offices, five overseas Legal Attache offices, other government agencies such as NASA, as well as the Royal Canadian Mounted Police. Reflecting the extraordinary level of cooperation on these investigations, on April 15, 2000, the Canadian officials arrested a juvenile charging him with one of the attacks.

Curador: On March 1, 2000, a computer hacker using the name, "Curador", allegedly compromised multiple E-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers. Thousands of credit card numbers and expiration dates were posted to various Internet websites. On March 9, 2000, InternetNews reported that Curador stated, "Law enforcement couldn't hack their way out of a wet paper bag. They're people who get paid to do nothing. They never actually catch anybody." After an extensive international investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (UK) Police Service in a search at the residence of Curador; Curador, age 18, was arrested in the UK, along with an apparent co-conspirator under the Computer Misuse Act 1990. Under United Kingdom law, both males have been dealt with as adults. Loss estimates are still being determined.

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of

law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Burns: In August 1998, the FBI initiated an investigation on an individual only known as "zyklon," who conducted numerous computer intrusions to various computer systems causing damages to websites and system files. The case was worked in cooperation with the Virginia State Police. The investigation identified zyklon to be Eric Burns of Shoreline, Washington. In February 1999, following an execution of a search warrant, Burns confessed to the intrusions. In May 1999, Burns also gained unauthorized access and defaced the webpage for the White House website. At that point the FBI began working with the U.S. Secret Service on the case. In September 1999, Burns pleaded guilty to one count for violation of Title 18 USC Section 1030 (Computer Fraud and Abuse) for one of the 1998 intrusions. In the plea agreement, Burns also admitted his criminal activity into several other intrusions including the White House website. In November 1999, Burns was sentenced to 15 months in prison, 3 years supervised release and $36,240 in restitution and a $100 fine.

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

Mewhiney: Throughout 1996, National Oceanic and Atmospheric Administration (NOAA) suffered several computer intrusions which were also linked to intrusions occurring a the National Aeronautics and Space Administration (NASA). These computer intrusions continued through 1997. The FBI worked the case jointly with NOAA, NASA, and the Canadian authorities and identified the subject, Jason G. Mewhiney, who resided in Canada. The original damage assessment that Mewhiney had caused, exceeded $40,000. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, Mewhiney pleaded guilty to 12 counts of intrusions which included violations spanning from May 1996 through April 1997, of destroyed/altered data and intrusions with the intent to damage. In the Canadian Superior Court of Justice, Mewhiney was sentenced to 6 months in jail for each of the counts to run concurrently.

Bliss: In February, 1998, the FBI opened an investigation to assist the U.S. Air Force and U.S. Navy regarding multiple computer intrusions. The case was worked jointly with the U.S. Naval Criminal Investigative Service and Florida State Attorney's Office in Jacksonville, FL. The subject was identified as Jesse Le Bliss, a student of the University of North Florida. On August 21, 1998, Bliss pleaded guilty to one felony count for violation of Florida State Statute 815.06 entitled, Offenses Against Computer Users. On September 19, 1998, Bliss was sentenced in the Fourth Judicial Circuit, State of Florida, to six months house arrest followed by three years probation, 200 hours of community service, and a written letter of apology to the Commandant of the United States Marine Corps.

CD Universe: One pending case being worked by the FBI's New Haven Division and the U.S. Secret Service has been widely reported in the press, due to statements made to reporters by the alleged perpetrator. In December 1999, the FBI's New Haven Division opened a case into intrusions into the computers of CD Universe, an on-line music seller, and the theft of customers' credit card numbers and a related extortion threat. Because of the credit card aspect, the FBI called the USSS to ask if USSS wanted to investigate jointly. The USSS declined. In January 2000, the New York Times ran a front page story about the case, based on conversations between the reporter and the alleged perpetrator. Subsequently, USSS called the FBI back and requested to work the case jointly. That case is still pending.

Other

There are other investigations that are being conducted with other agencies, however further details may adversely impact the investigation due to their pending status. There are currently 47 pending investigative cases which are being worked jointly between the FBI and the multiple entities of the Department of Defense. An additional 58 cases were investigated jointly with other entities that are now in closed status.

2. If some of the referred cases are potential violations that are traditionally enforced and investigated by other agencies, please describe your mechanisms and procedures that allow for cyber investigations to be conducted by those particular law enforcement agencies (other than the FBI).

The primary statute used by the FBI in computer intrusion investigations is Title 18, USC, 1030. Under this statute, the FBI has broad authority to investigate computer crime offenses. In instances where the computer crime does not meet FBI jurisdiction, the local FBI field office will refer the complainant to the appropriate law enforcement agency (federal, state, or local) which has authority to conduct the investigation. On other occasions, the FBI may continue to work a matter jointly with another law enforcement agency, even if they do not have primary jurisdiction, to provide needed resources and technical expertise. FBI field offices develop liaison contacts with state and local agencies investigating similar violations under state statutes and complaints are disseminated through these liaison contacts. The above cited credit card case is an example of

how the FBI field offices make direct contact with their counterpart field offices, such as US Secret Service, to coordinate aspects of an investigation.

3. Please specifically cite the number of NIPC referred cases that have a direct impact or posed a threat on the nation's critical infrastructures.

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus, there is no methodology to determine which cases ultimately involve a threat to our nation's critical infrastructure.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

4. Please describe the job description and agency of any state and local law enforcement officials currently assigned to NIPC on a full time basis at FBI Headquarters.

The FBI currently has one local law enforcement officer assigned to the NIPC. He is from the Tuscaloosa County Sheriffs Department and his principal job is to work on outreach initiatives

5/24/02 Release - Page 398

to state and local law enforcement as part of the FBI's responsibility as the "Lead Agency" to work with the "Emergency Law Enforcement Services Sector" under PDD-63. He has also participated in the delivery of training to field investigators under our Key Asset Initiative. This representative replaced an earlier representative from the Oregon State Police, who rotated back to his home agency. The NIPC is also in discussions with several Washington, D.C. area police departments about having officers detailed to the NIPC on a full- or part-time basis.

5. Please describe any private sector representatives, past or present, who voluntarily participate in the Center to facilitate sharing of information between NIPC and the private infrastructure owners and operators.

The NIPC works on a daily basis with private sector representatives to share information. This occurs through such initiatives as InfraGard, which provides information to infrastructure owners and operators on a daily basis, and the pilot project for Indications and Warning that the NIPC has established with the electrical power sector under the auspices of NERC, and the Key Asset Initiative. It also occurs on a case by case basis as we disseminate targeted or general alerts or warnings to industry. The NIPC also works closely with private sector contractors who assist with technical analysis and information sharing.

In addition, the NIPC is working with the Information Technology Association of America to bring private sector representatives into the Center for a period of time as "detailees." That is part of a cybercrime initiative sponsored by the ITAA and the Attorney General.

6. Please describe any private sector representatives that are hired and paid by NIPC funds.

The NIPC has hired contractors to support our work in analyzing cyber intrusions into the infrastructures as well as to provide technical support to our investigations. In addition, a representative from Sandia National Laboratories, has been working at the Center. The NIPC has been reimbursing the Department of Energy under the Interagency Personnel Act for the cost of this detailee's contract.

7. On page 16 of your written testimony, you state: "the FBI, on behalf of the law enforcement community should enhance its technical capabilities (encrypted evidence)." Shouldn't all law enforcement agencies, from federal to state require this capability to accomplish the NIPC mission ?

As noted on page 16 of the written testimony, the law enforcement community is extremely concerned about the serious public safety threat posed by the proliferation and use of strong, commercially-available encryption products that do not allow for law enforcement access to the plaintext of encrypted, criminally-related evidence obtained through court-authorized electronic surveillance and/or search and seizure. The potential use of such non-recoverable encryption products by a vast array of criminals and terrorists to conceal their criminally-related communications and/or electronically stored information poses an extremely serious threat to

public safety and national security.

In order to address this serious threat and as noted in the written testimony, it is imperative that law enforcement enhance it technical capabilities in the area of plaintext access to encrypted evidence. As part of the government's approach to the encryption issue, the Administration has expressed support for and has proposed the creation of a law enforcement Technical Support Center within the FBI for the purpose of providing the entire law enforcement community with urgently needed plaintext access technical capabilities necessary to fulfill its investigative responsibilities in light of the proliferation of strong, commercially-available encryption products within the U.S. In fact, included in the Administration's Cyberspace Electronic Security Act of 1999 which was forwarded to the Congress last September is a provision that authorizes to be appropriated $80 million to the FBI for the creation of the Technical Support Center, which will serve as a centralized technical resource for federal, state and local law enforcement in responding to the ever increasing use of encryption by subjects of criminal cases.

The TSC is envisioned as an expansion of the FBI's Engineering Research Facility (ERF) to take advantage of ERF's existing institutional and technical expertise in this area. This approach represents a cost effective, non-duplicative and efficient means of provide every U.S. law enforcement agency with access to technical capabilities needed to address lawfully seized encrypted evidence and is supported by the International Association of Chiefs of Police, the National Sheriff's Association and the National District Attorney Association as well as the Information technology industry.

8. Please describe which agencies were in the past participating in the NIPC, but are no longer members. Describe the reasons given by those agencies to the FBI for their withdrawal from participation.

One of the difficulties in attempting to operate an interagency Center is ensuring that all relevant agencies participate. Agencies have not received direct funding to participate in the Center, and so must take detailees to the NIPC out of existing personnel resources. In addition, personnel with cyber expertise are unfortunately in very short supply, meaning that agencies must commit to take scarce resources and send them outside their agencies. Despite these impediments, numerous agencies have sent detailees to the NIPC, including: Defense/Office of the Secretary of Defense; Central Intelligence Agency; National Security Agency; Air Force Office of Special Investigations; U.S. Navy; U.S. Army; U.S. Postal Service; Defense Criminal Investigative Service; General Services Administration; U.S. Air Intelligence Agency; Department of Commerce, and the Tuscaloosa, AL Sheriff's office. In addition, we have foreign liaison representatives from two allied countries who assist in coordinating international activities with our counterparts. A representative from FAA is also scheduled to start at the end of June. Additional representative from DoD, CIA, and NSA are also slated to arrive in the near future. We are also expecting representatives from local Washington area police departments on a part-time basis.

5/24/02 Release - Page 400

Some agencies were represented earlier but do not currently have representatives. Circumstances necessitated the recall of the first State Department representative. State agreed to do so, and has committed to NIPC that it would replace him with two new representatives. DoE's first representative rotated back after more than two years. NIPC's understanding as to why this representative rotated back is that he was at NIPC for a lengthy time and was needed at DoE headquarters to assist in a DOE reorganization. DoE has committed to replacing that detailee.

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has not yet committed to replacing them. Secret Service has not provided any written explanation for this, but in oral discussions, Secret Service officials stated that USSS was not getting additional funding for its electronic crimes program despite its participation in NIPC; the FBI was receiving more media attention in the cyber crime area; and NIPC had not "referred" cases to Secret Service for investigation. NIPC offered any support it could give to Secret Service in addressing budget requests; noted that NIPC public statements often referred to partnership with USSS; and offered to do more to support USSS initiatives with public statements and case analyses. NIPC also stated (as discussed further below) that its role is not to create and "refer" cases; rather, cases generally originate in Field Offices, and FBI and Secret Service field offices frequently work computer crime cases together.

NIPC fully recognizes the value other agencies bring to the cyber crime and infrastructure protection mission. That is why NIPC is an interagency Center, and has senior managers from other agencies in addition to investigators and analysts. For instance, the NIPC Deputy Director is from DoD/OSD; the Section Chief of the Analysis and Warning Section is from CIA; the Assistant Section Chief of the Computer Investigations and Operations Section is from Air Force OSI; the Unit Chief of the Analysis and Information Sharing Unit is from NSA; and the Unit Chief of the Watch and Warning Unit is from the U.S. Navy. Secret Service formally occupied the position of Assistant Section Chief of the Training, Outreach, and Strategy Section. Recognition of the need for other agency participation is also what drives NIPC to continually seek additional representatives from other agencies. It is also reflected in the numerous joint investigations that NIPC and FBI Field Offices have been involved in with other agencies (as discussed further below).

Senator Leahy:

1. Can an attempt to commit a violation of 18 U.S.C. § 1030 (a)(5) currently be prosecuted under the attempt provision found in 18 U.S. C. § 1030(b), even if the attempt does not result in loss of at least $5,000 or cause one of the other results listed in § 1030 (e)(8)?

The question calls for an answer interpreting prosecution authority under statute, and as such, is more appropriately propounded to the Department of Justice. As a general rule, however, the FBI understands that, under certain factual circumstances, 18 U.S.C. § 1030(b) does allow for the prosecution of violations of 18 U.S.C. § 1030(a)(5) even if the attempt does not result in a loss of at least $5,000 where evidence demonstrates the offender's specific intent was to cause a loss

5/24/02 Release - Page 401

in excess of $5,000.

2. If an attempt cannot be so prosecuted, would amending the statute so that the aggravating factors included in the definition of "damage" in 18 U.S.C. §§ 1030 (e)(8)(A)-(D) are instead moved to be elements of the offense under § 1030 (a)(5) change that result?

The question calls for a hypothetical interpretation of a statutory amendment as applied through the substantive case law of "attempt," and should be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI does not understand that elevating the definitional elements of the term "damage" to become substantive elements of section 1030 offenses will, in all circumstances, resolve the attempted offense issues generated by the facts of most investigations. Instead, the FBI favors an approach which would combine a restructuring of the elements of the definition of "damage" into the penalty provisions of section 1030(c) with the creation of a lesser offense for those circumstances where damages of $5,000 or more cannot be substantiated. The FBI believes that some unauthorized access intrusions into computers affecting interstate commerce (i.e., protected computers) are so inherently violative as to justify Federal criminal sanctions even where there is no change affecting the integrity or availability of data or where the actual damages suffered do not attain the $5,000 threshold. The intentional unauthorized computer intrusion into the privileged and private medical records of citizens is but one such example. Such a statutory approach as has been suggested by DoJ's Computer Crime and Intellectual Property Section (CCIPS) would create a lesser included misdemeanor offense where the $5,000 threshold is not, in fact, demonstrated and would provide jurors in cases involving damages close to the threshold a legitimate alternative for otherwise violative behavior.

3. If a definition of "loss" were added to § 1030(e) to define loss as "the reasonable cost to any victim of responding to the offense, conducting a damage assessment, restoring data, programs, systems or information to their condition prior to the offense and any revenue lost or costs incurred by the victim as a result of interruption of service," would the $5,000 threshold be easier to meet than under current law?

The FBI favors any amendments which allow for the increased inclusion of any costs, losses or other expenditures that a victim would not have reasonably incurred but for the violation regardless of whether those losses resulted from an actual interruption of service. The FBI favors such a definition which would also include, if reasonable, the cost of system reconfiguration related to deterring or eliminating similar future violations.

4. With respect to violations of § 1030(a)(5)(A), is it your understanding that each separate "transmission" could form the basis of a separate count? Similarly, with respect to violations of §§ 1030(a)(5)(B)-(C), is it your understanding that each separate "intentional access[ ] " could form the basis of a separate count?

The question calls for an interpretation of a statute applying the substantive case law of

5/24/02 Release - Page 402

what constitutes "criminal episode," and related concepts of what constitutes appropriate "joinder," or "severance" under the Federal Rules of Criminal Procedure and should more appropriately be directed to the Department of Justice for a detailed and definitive response. As a general matter, however, the FBI understands that whether a single computer transmission of malicious code under section 1030(a)(5) may form the basis for a single count under an indictment will, in large measure, turn upon the unique facts of any given investigation. Whether a single transmission of a self-replicating, self transmitting destructive computer virus constitutes one transmission, and therefore one count, or thousands of transmissions intentionally effectuated by chain reaction, and therefore thousands of counts, may turn upon an evaluation of numerous factors not the least of which would include the object and intent of the offender/transmitter, the design of the code, the reasonable foreseeability of re-transmission and, as a practical matter, the ability to track, gauge and prove the re-transmission. Similarly, whether, in a computer network environment, the repeated unauthorized accessing of a computer in violation of section 1030(a)(5)(B)-(C), which accessing is temporally related, will, as a practical matter, frequently turn upon the configuration of the network and its security and banner system, to name but a few factors.

5. Are you aware of any cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. § 1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. § 5G1.2, which provide that sentences on multiple counts may be imposed consecutively to the extent necessary to produce a combined sentence equal to the total punishment called for by the guidelines?

The NIPC referred this question to the Department of Justice Computer Crimes and Intellectual Property Section for input. The Department reported that it could recall no cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. § 1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. § 5G1.2.

6. Please explain the reason, if any, to continue the codification of the work-sharing agreement between the Secret Service and the Federal Bureau of Investigation found in § 1030(d)?

In 1996, Congress specifically limited the Secret Service's authority to investigate crimes under 18 U.S.C. § 1030 to those offenses under subsections (a)(2)(A) and (B), (a)(3), (a)(4), (a)(5) and (a)(6). The Senate Report accompanying the 1996 amendment explained that:

> [t]he new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal

5/24/02 Release - Page 403

Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

S. Rep. No. 357, 104th Cong., 2d Sess. 13 (1996).

Inherent in the 1996 changes was the recognition that the statute was being amended to reflect the respective investigative jurisdictional limits existing at that time. It was clear at that time that the jurisdiction of the Secret Service, found at 18 U.S.C. § 3056, did not encompass the types of offenses described in Section 1030 (a)(1), (a)(2)(C), or (a)(7).[1] Given that there have been no additional grants of general investigative jurisdiction to the USSS since that amendment, it is not clear why the USSS's jurisdiction over computer crimes under Section 1030 should be expanded. The theft of National Security information which is the type of information Section 1030(a)(1) was intended to address has never been the subject of USSS jurisdiction. In addition, the types of crimes contemplated by 1030(a)(2)(C) and (a)(7), as recognized by the legislative history, have traditionally been investigations solely in the province and expertise of the FBI.

The 1996 provision is an explicit effort by Congress to address the criminal offenses at issue through a division of labor primarily determined by investigative responsibility and expertise. Any reversion to the pre-1996 jurisdictional provisions raises serious issues and concerns about the utilization of resources and proper coordination. Concurrent jurisdiction would result in a duplication of efforts that would waste resources and encourage independent investigations by separate agencies at the expense of coordinated joint efforts. Indeed, given the decision by Secret Service to refrain from participation in the National Infrastructure Protection Center (NIPC) (both by detailing personnel and providing investigative information from its cases) despite a mandate from the President to do so under PDD-63, expanding USSS's cyber jurisdiction at this time would result in a fractured approach to sensitive intrusion investigations involving espionage, extortion, and other serious matters.

7. The FBI has limited authority to issue administrative subpoenas in certain cases, such as federal health care fraud or sexual exploitation or other abuse of children. Since cybercrime cases are criminal in nature, is the FBI able to obtain documents relevant to the investigation with grand jury subpoena? To the extent that documents obtained with a

---

[1] "Under the direction of the Secretary of the Treasury, the Secret Service is authorized to detect and arrest any person who violates --

(1) section 508, 509, 510, 871, or 879 of this title or, with respect to the Federal Deposit Insurance Corporation, Federal land banks, and Federal land bank associations, section 213, 216, 433, 493, 657, 709, 1006, 1007, 1011, 1013, 1014, 1907, or 1909 of this title;

(2) any of the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; or

(3) any of the laws of the United States relating to electronic fund transfer frauds, credit and debit card frauds, and false identification documents or devices; except that the authority conferred by this paragraph shall be exercised subject tot he agreement of the Attorney General and the Secretary of the Treasury and shall not affect the authority of any other Federal law enforcement agency with respect to those laws.

5/24/02 Release - Page 40

grand jury subpoena need to be shared with third-party experts, can permission be obtained to do so under Federal Rule of Criminal Procedure 6(e)(3)?

Generally speaking, a "governmental entity" is authorized under 18 U.S.C. 2703 (b) (1) (B) to obtain the contents of an electronic communication in *remote computer storage* with prior notice, as delimited in 18 U.S.C. 2703(b) (2), by using an administrative or grand jury subpoena. A governmental entity is also authorized under 18 U.S.C. 2703(c)(1)(C) to obtain certain subscriber or customer information from a provider of electronic communication services or remote computing service, by using an administrative, grand jury, or trial subpoena, or as otherwise permitted under 18 U.S.C. 2703 (c)(1)(B). The Electronic Communications Privacy Act (ECPA) does not itself identify which federal agencies qualify as "government entities" authorized to issue administrative subpoenas. Currently, the FBI is authorized to issue administrative subpoenas in cases involving health care fraud under 18 U.S.C. §3486 and in cases involving child pornography and sexual solicitation under 18 U.S.C. §3486A. Unfortunately, there does not currently exist a statute authorizing or designating the FBI as a "governmental entity" authorized to issue administrative subpoenas for violations of 18 U.S.C. § 1030 or other crimes of fraud increasingly committed by or facilitated through the use of a computer. The absence of such a statute impedes FBI efforts to accelerate an effective response to cyber crime.

While helpful, the use of grand jury subpoena to acquire minimally intrusive transactional information (e.g., so-called "header information" such as "to" or "from") or subscriber information (e.g., the name and address of the owner of an Internet screen name) is frequently a cumbersome and time consuming process especially in investigations where time is of the essence or where the information sought is from an unusually large number of providers. Some circumstances may dictate seeking express court authorization under the provisions of Federal Rule of Criminal Procedure 6(e)(3)(C) for disclosure to non-government experts who may not qualify as personnel assisting the attorney for the government in the investigation before the grand jury. In many cases, the practical concerns of delay and coordination with other agencies and courts further stymies government's ability to provide a timely response to imminent criminal behavior.

The FBI supports an expansion of its statutory authority to issue administrative subpoena under the Electronic Communications Privacy Act for any violation of law within the FBI's existing criminal investigative jurisdiction. The FBI's experience to date in the issuance of administrative subpoena in the areas of health care fraud and child exploitation crimes demonstrates that it can responsibly limit and control the exercise of this authority.

8. Denial of service attacks are increasing exponentially. According to the FBI, these attacks involve the placement of tools such [as] Trinoo, Tribal Flood net, TFN2K or Stechenldraht on unwitting victim systems, which then send messages upon remote command to a targeted computer system until that system is overwhelmed and essentially shut[s] down. In order to document in real-time the remote command being given and the triggering of the message flood to the target system, is law enforcement currently required to obtain a wiretap order since the unwitting victim system is not a "party to the communication" authorized to grant

consent to electronic surveillance? Would an exception to the wiretap law to allow the unwitting victim system operator to grant consent to electronic surveillance be helpful to law enforcement?

The question calls for an interpretation of a statute which would more appropriately be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI understands that: 1) the provisions of 18 U.S.C. §2511(1)(a) prohibit all interceptions unless expressly authorized elsewhere in the Act; 2) the provisions of 18 U.S.C. §2511(2)(a)(i) authorize a provider of wire or electronic communication services to intercept communications on their system, not because they are parties to those communications, but as "is a necessary incident to the rendition of [that] service or to the protection of the rights or property of the provider....;" 3) many providers (especially start-up Internet services) may not have the necessary tools or expertise to adequately track, document or halt an intruder in their system and, more perhaps more significantly, no providers have compulsory process to facilitate disclosure of transaction and subscriber information from other providers which is necessary to identify the source of an attack; 4) 18 U.S.C. §2511(2)(a)(i) does not permit law enforcement to conduct an interception (without a court order) even upon a provider's express request when the provider's system has been invaded or trespassed upon by a hacker, and 5) as a result of this quandary, and in order to ensure that evidence obtained will subsequently be held admissible, law enforcement is required to obtain a court order in order to enable it to actively work in conjunction with the provider.

Given the high level DOJ approval that is required for Title III Interception applications, the necessary generation of paperwork, and the time needed by the reviewing court, significant delay can occur before law enforcement can provide an effective response to a hacker or DDOS event. This anomaly in the law creates an untenable situation whereby providers are sometimes forced to sit idly by as they witness hackers enter and, in some situations, destroy or damage their systems and networks while law enforcement begins the detailed process of seeking court authorization to assist them. In the real world, the situation is akin to a homeowner being forced to helplessly watch a burglar or vandal while police seek a search warrant to enter the dwelling. For these reasons, the FBI favors enactment of a statutory exception under 18 U.S.C. §2511 which would expressly authorize law enforcement to assist such providers by intercepting the communications of a computer user/trespasser (the transmissions to and from the user/trespasser) BUT ONLY upon the voluntary, written consent of a service provider after that provider has made an initial determination that the user/trespasser is, in fact, not authorized to be on the system or network. Such an exception to the general interception prohibition would accelerate exponentially law enforcement's ability to respond to such hacker incidents and would be a significant step toward ensuring the security and integrity of the Nation's critical infrastructure.

1. Is law enforcement currently required to obtain a wiretap in order to document in real-time the remote commands being given to a target system?

potential exception to this would be certain pen register-based approaches employed by service providers in switch-based solutions, where post-cut-through dialing (including post-cut- through signaling) may not be provided to law enforcement. This circumstance is currently a subject of review by the FCC under rule making implementing CALEA, and regarding which we anticipate a resolution in the near future.) The distinction between a pen register device on a telephony service and a clone pager (or pager interception) is that a pen register is employed to capture dialed numbers which are used to set up a call. Hence, in the overwhelming majority of instances where pen registers are used the information captured is simply signaling information used to set up a call. By comparison, pager interceptions are employed to capture the information received by a pager which, in all instances, constitute the content or message of the call. Consequently, the law has historically distinguished the legal processes required for these two types of acquisitions (i.e., pen register authority vs Title III authority, respectively).

Pen register efforts in the data network area work somewhat differently. The most basic reason for this is because the services (e.g., email, web-based mail, voice over IP) and applications (e.g., Internet Chat, File Transfer) transmitted over data networks are somewhat different. Some of these services and applications lend themselves to precise ways of capturing (i.e., recording) call identifying and signaling information only while others make the process of differentiating signaling information from call content more difficult.

9(B) Section 3121(c) of title 18, United States Code, requires government agencies authorized to use pen registers to "use technology reasonably available...that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Please describe the technology and methodology currently employed to comply with this statutory requirement.

Pen Register devices on telephony services continue to operate as they have for decades. Stated differently, since the enactment of CALEA, there has been no change in technology or pen register equipment for telephony that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

As stated above, pen register efforts in the data network area work somewhat differently, and there, where technology that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information is reasonably available, it is employed. For example, the FBI employs pen register devices to capture Internet Protocol (IP) addresses. Since data networks typically use well-established layered protocols, FBI tools are capable of restricting the information captured to the IP address.

10. Section 3121(a) of title 18, United States Code, requires a court to authorize the use of a pen register if the court finds that the government attorney has certified that the information likely to be obtained by "such use is relevant to an ongoing criminal investigation." The certification by the government attorney is, in turn, made under oath and penalty of perjury,

under section 3122.

(A) Is the government attorney required to describe to the court in the application for a pen register the factual basis for the attorney's certification that "such use is relevant to an ongoing criminal investigations"?

(B) As a matter of regular practice, do government attorneys or State law enforcement or investigative officers making applications for pen registers describe for the court the factual basis for the certification that "such use is relevant to an ongoing criminal investigation" or does this practice vary?

(C) What procedures, including audits or internal reviews, are in place to ensure that government attorneys and State law enforcement or investigative officers comply with the statutory standard and have the necessary factual basis for making the application, particularly in those districts where the practice in applying for pen register orders is not to describe for the court the factual basis for certification?

(D) Should the court, rather than governmental attorneys or State law enforcement or investigative officers, be given the authority to make the factual finding that "information likely to be obtained by such installation and use [of a pen register] is relevant to an ongoing criminal investigation," and if not, please explain why?

Several of the questions call for or implicate an interpretation of statute which would more appropriately be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI understands the Supreme Court has expressly ruled that "the installation of a pen register ...[is] not a "search" within the meaning of the Fourth Amendment and therefore its use does not violate the Constitution." Smith v. Maryland, 442 U.S. 735, 745-46, 99 S.Ct. 2577, 2583 (1979). Given the lack of an expectation of privacy at stake in the limited, non-content information garnered through the use of pen registers, the Courts have held that the limited judicial review role delineated by 18 U.S.C. §3121 *et seq.* is Constitutional and is intended to safeguard against the purely random use of pen register devices by ensuring compliance with the statutory requirements established by Congress. *See United States v. Hallmark*, 911 F.2d 399, 401-402 (10th Cir. 1990).

Pen Register certifications by government attorneys are drafted and filed by attorneys of the Department of Justice and not, at the Federal level, by Special Agents of the FBI. Questions regarding the substance of such certifications would more appropriately directed to the Department of Justice for a more definitive response. As a general matter, however, it is the FBI's experience that the degree to which a pen register application to the Court discloses the underlying factual basis for the attorney's certification turns, in large measure, upon the nature of the statutory offense which is the focus of the investigation. Whereas section 3123(b)(1)(D) requires that all pen register orders contain a "statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates," it follows that the application required by section 3122(b)(2) contain

such a statement within the attorney's certification and it is the FBI's experience that this is commonly the case. Depending upon the nature of the offense described in the certification, the underlying basis for the certification can, and in most instances will be readily apparent. Thus, in telemarketing fraud investigations, the obvious underlying basis is that the offenders are using the telephone to solicit victims. Similarly in narcotics and conspiracy to commit narcotics violations, the reliable and common sense inference is clearly that telecommunications are being used to facilitate the possession, distribution and sale of controlled substances in violation of Title 21 of the United States Code. Even in investigations involving computer hacking in violation of the Computer Fraud and Abuse Act (18 U.S.C. §§1030 *et seq.*), it requires little thought or imagination to understand the underlying basis for the request.

The FBI also understands that the sole basis for obtaining a pen register order is to further a criminal investigation by generating reliable admissible evidence. An attorney who falsely or recklessly certifies an application under oath pursuant to 18 U.S.C. §3122(b)(2) does so at his/her peril subject to sanction, disbarment and prosecution. Furthermore, an attorney who so falsely certifies such an application has no way of knowing the subsequent course and outcome of the investigation. Frequently, information received from a pen register is consolidated with other investigative information and is submitted in subsequent, more detailed applications to the Court such as search warrant applications or wiretap applications. In the unlikely event that an attorney for the government were to submit a false certification to the court in support of a pen register application, the lack of any nexus between the named subjects of the investigation, the "statement of the offense," and the attorney's certification that the information likely to be obtained from the devise's use is relevant to an ongoing criminal investigation would, in many instances, reveal itself either in subsequent applications to the Court for search warrants or wiretaps, or in discovery incident to prosecution. The dearth of such empirical or anecdotal evidence demonstrating inappropriate or false certification of applications by attorneys for the government demonstrates that the certification obligation is conscientiously fulfilled.

11. You have testified that information theft and financial fraud perpetrated online have caused the most severe financial losses, "put at $68 million and $56 million respectively." In fact, you have identified "use of the Internet for fraudulent purposes" as "one of the most critical challengers facing the FBI and law enforcement in general.: Appreciating this challenge, I have urged that the Congress be careful in considering legislation, such as H.R. 1714, " The Electronic Signatures in Global and National Commerce Act," to ensure that consumers are adequately protected in the online environment. This bill has passed the House of Representatives and is currently the subject of a conference with the Senate.

(A) The National Association of Attorneys General has commented on H.R. 1714, stating that the bill's provisions permitting storage of only synopses of documents that "accurately reflect" originals, even where the law otherwise requires retention of original documents, "has the strong potential to negatively impact law enforcement discovery of document." Do you agree and, if not, please explain why?

(B) H.R. 1714 would require that state enactments of the Uniform Electronic Transactions Act (UETA) "be consistent with" the House bill, resulting in federal preemption of any state exemption from the presumption of validity of electronic signatures and transactions that is not authorized in the House bill. The National Association of Attorneys General has opined that this broad federal preemption would "unduly hinder the ability of the states to protect their citizens against consumer fraud." If States are hindered in combating consumer fraud, would the FBI's job in protecting the public from fraudulent online practices be made more difficult?

On its face, the provisions of H.R. 1714 which allow for the electronic storage of contracts, agreements and records are unrelated to earlier provisions of the bill delineating what types of legal documents may be executed by electronic signature. To the extent that Section 101(c)(1)(c) could be interpreted as allowing for the electronic imaging and storage as an electronic record of written contracts or agreement, the tangible originals of which would otherwise be required by law to be maintained in tangible form, then, there could exist the potential to negatively impact certain law enforcement investigations relating to such documents. At a minimum, the supplanting of tangible originals (otherwise legally required to be maintained in tangible form) with electronic images depicting the originals, when coupled with destruction of the originals, would eliminate or complicate handwritten signature analysis and render null the possibility of recovering fingerprints or other trace evidence from the surface of originals. By the same token, the provisions of section 101(c)(2) which exempt from retention data relating to the communication or receipt of any contract, agreement or record electronically recorded, could, in the context of electronically executed contracts, complicate or eliminate law enforcement efforts in tracing the source of transmission of fraudulent transactions or the location and identity of co-conspirators or even other victims. The continued trend toward electronic, paper-less execution of commercial transactions (which is admittedly so critical to the continued evolution and expansion of the Internet) when coupled with 1) the growing ability of criminals to utilize encryption to restrict law enforcement's ability to recover crucial inculpatory evidence, and 2) the absence of any preeminent public key, or private signature verification entity or procedure complicates the efforts of the FBI and state law enforcement to protect the public from on-line fraud.

1. synopses only of documents can negatively impact law enforcement?

The review of complete and accurate records is often necessary in law enforcement's effort to help investigate crime. All records management and retention policies therefore can be said to have an effect on law enforcement, and those policies which do not require that information be maintained, at least in theory, can negatively impact law enforcement's discovery of that information.

2. If states are hindered . . .

The FBI believes that since States are the primary responders to crime in our country, if the States are hindered in combating consumer fraud, then the FBI's job in protecting the public from fraudulent online practices wold be made more difficult.

Citation Search Result Rank 4 of 18 Database
U.S. Attys. Man. 9-7.010 USAM
U.S. Attorney's Manual 9-7.010

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-7.000 ELECTRONIC SURVEILLANCE
September 1997

9-7.010 Introduction

This chapter contains Department of Justice policy on the use of electronic surveillance. The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") are codified at 18 U.S.C. § 2510, et seq. Because of the well-recognized intrusive nature of many types of electronic surveillance, especially wiretaps and "bugs," and the Fourth Amendment implications of the government's use of these devices in the course of its investigations, the relevant statutes (and related Department of Justice guidelines) provide restrictions on the use of most electronic surveillance, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception.

Chapter 7 contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance. Additional information concerning use of the various types of electronic surveillance is also set forth in the Criminal Resource Manual at 27.

Attorneys in the Electronic Surveillance Unit of the Office of Enforcement Operations, Criminal Division, are available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder. Interceptions conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, which is codified at 50 U.S.C. § 1801, et seq., are specifically excluded from the coverage of Title III. See 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

9-7.010
U.S. Attys. Man. 9-7.010
END OF DOCUMENT

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

Citation Search Result Rank 5 of 18 Databas
U.S. Attys. Man. 9-7.100 USAM
U.S. Attorney's Manual 9-7.100

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-7.000 ELECTRONIC SURVEILLANCE
September 1997

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders--Overview and History of Legislation

To understand the core concepts of the legislative scheme of Title III, one must appreciate the history of this legislation and the goals of Congress in enacting this comprehensive law. By enacting Title III in 1968, Congress prohibited private citizens from using certain electronic surveillance techniques. Congress exempted law enforcement from this prohibition, but required compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted Many of the restrictions upon the use of electronic surveillance by law enforcement agents were enacted in recognition of the strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution. See, e.g., Katz v. United States, 389 U.S. 347 (1967). Still, several of Title III's provisions are more restrictive than what is required by the Fourth Amendment. At the same time, Congress preempted State la in this area, and mandated that States that sought to enact electronic surveillance laws would have to make their laws at least as restrictive as the Federal law.

One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level Justice Department officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

U.S. Attys. Man. 9-7.100

TEXT
General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11), discussed at USAM 9-7.111.)

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added a new category of covered communications, i.e., "electronic communications," which would now be protected, and whose interception would be regulated, by Title III. Electronic communications are those types of non-oral or wire communications that occur inter alia, over computers, digital-display pagers, and facsimile ("fax") machines. See 18 U.S.C. § 2510(12).

Although the 1986 amendments permit any government attorney to authorize the making of an application to a Federal court to intercept electronic communications to investigate any Federal felony (18 U.S.C. § 2516(3)), the Department of Justice and Congress agreed informally at the time of ECPA's enactment that, for a three-year period, Department approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that period, the Department rescinded the prior approval requirement for the interception of electronic communications over digital-display paging devices, but continued the need for Department approval prior to application to the court for the interception of electronic communications over any other device, such as computers and fax machines. Applications to the court for authorization to intercept electronic communications over digital-display pagers--which are the most commonly targeted type of electronic communications--may be made based solely upon the authorization of a United States Attorney. See 18 U.S.C. § 2516(3).

Because there are severe penalties for the improper and/or unlawful use and disclosure of electronic surveillance evidence, including criminal, civil, and administrative sanctions, as well as the suppression of evidence, it is essential that Federal prosecutors and law enforcement agents clearly understand when Departmental review and approval are required, and what such a process entails. See 18 U.S.C. §§ 2511, 2515, 2518(10), and 2520.

See the Criminal Resource Manual at 31, for citations to relevant legislation.

9-7.100
U.S. Attys. Man. 9-7.100
END OF DOCUMENT

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

Citation Search Result Rank 6 of 18 Database
U.S. Attys. Man. 9-7.110 USAM
U.S. Attorney's Manual 9-7.110

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-7.000 ELECTRONIC SURVEILLANCE
September 1997

9-7.110 Format for the Authorization Request

When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings, which include:

A. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application;

B. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications; and

C. A set of orders to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application, including appropriate redacted orders to be served on any relevant providers of "electronic communication service" (as defined in 18 U.S.C. § 2510(15)).

9-7.110
U.S. Attys. Man. 9-7.110
END OF DOCUMENT

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

Citation Search Result Rank 16 of 18 Database
U.S. Attys. Man. 9-60.202 USAM
U.S. Attorney's Manual 9-60.202

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-60.000 PROTECTION OF THE INDIVIDUAL
September 1997

9-60.202 Illegal Electronic Eavesdropping--Prosecution Policy

The criminal prohibitions against illegal electronic eavesdropping contained in Title III are part of the same act which permits federal law enforcement officers to engage in court-authorized electronic surveillance. Congress viewed the criminal sanctions and the court authorization provisions as two sides of the same coin. The retention of the government's authorization to engage in court-authorized electronic surveillance may depend on its vigorous enforcement of the sanctions against illegal electronic eavesdropping. Accordingly, it is the Department's policy to vigorously enforce these criminal prohibitions.

The Department's overall prosecutive policy under 18 U.S.C. $ 2511 is to focus primarily on persons who engage or procure illegal electronic surveillance as part of the practice of their profession or as incident to their business activities. Less emphasis should be placed on the prosecution of persons who, in the course of transitory situations, intercept communications on their own without the assistance of a professional wiretapper or eavesdropper. This does not mean that such persons are never to be prosecuted, but simply that this type of prosecution is not a major thrust of the Department's enforcement program.

Most illegal interceptions fall into one of five categories: (1) domestic relations, (2) industrial espionage, (3) political espionage, (4) law enforcement, and (5) intra-business. The largest number of interceptions, more than 75 percent, are in the domestic relations category. It is the Department's policy to vigorously investigate and prosecute illegal interceptions of communications which fall within the industrial and political espionage, law enforcement, and intra-business categories. Generally such violations will have interstate ramifications which will make federal prosecution preferable to state prosecution. Nevertheless, in cases where the federal interest is slight, it may be appropriate to defer to state prosecution.

Illegal interceptions arising from domestic relations disputes generally present less of a federal interest and, therefore, local prosecution is more appropriate. However, this does not mean that federal prosecutors should abdicate responsibility for prosecuting such interceptions. Indeed, in view of the preponderance of this kind of interception, no enforcement program can be effective without the initiation of some prosecutions for deterrence purposes. United States Attorneys should develop effective liaison with local prosecutors in order to convince them to shoulder their share of the burden.

Within the category of domestic relations violations, primary attention should be given to those instances in which a professional is involved, such as a private detective, attorney, moonlighting telephone company employee, and

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

U.S. Attys. Man. 9-60.202

TEXT
supplier of electronic surveillance devices. United States Attorneys should feel free to pursue these cases or refer them to local prosecutors; however, no professional should escape prosecution when a prosecutable case exists.

Domestic relations violations which do not involve a professional interceptor are the lowest priority cases for federal prosecution. Although local prosecution is normally preferable, when local prosecutors are unwilling to pursue the case, resort to federal prosecution may be appropriate. Nevertheless, violations of this type will sometimes prove to be of insufficient magnitude to warrant either federal or state prosecution. In such cases, other measures may prove sufficient, for example, a civil suit for damages (18 U.S.C. § 2520), suppression of evidence (18 U.S.C. § 2515), or forfeiture of the wiretapping or eavesdropping paraphernalia (18 U.S.C. § 2513).

Disturbed persons often suspect that they are the victims of illegal interceptions. Consequently, a complaint which is based solely on suspicious noises heard on the telephone normally does not merit further investigation if the initial line check fails to produce independent evidence of a tap.

9-60.202
U.S. Attys. Man. 9-60.202
END OF DOCUMENT

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

Citation Search Result Rank 17 of 18 Database
U.S. Attys. Man. 9-60.262 USAM
U.S. Attorney's Manual 9-60.262

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-60.000 PROTECTION OF THE INDIVIDUAL
September 1997

9-60.262 Prosecutive Policy--18 U.S.C. § 2512

Flagrant violators of 18 U.S.C. § 2512 should be prosecuted vigorously, especially violators who possess such devices in order to engage in electronic surveillance as a business.

Less culpable first offenders and those who violate the statute because of ignorance of the law may be appropriate subjects for more lenient disposition. In some cases a warning may be sufficient. Nevertheless, in all cases except, perhaps, for minor advertising violations, the United States Attorney's Office should require that the prohibited device either be surrendered voluntarily to the FBI or forfeited pursuant to 18 U.S.C. § 2513.

9-60.262
U.S. Attys. Man. 9-60.262
END OF DOCUMENT

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

b6-1 / b7c-1

From: [redacted] b6-1
To: b7c-1
Date: 7/20/00 6:20PM
Subject: Don Kerr's Testimony

b6-1
b7c-1 [redacted]

The revisions that I just gave you do not include a fix for the problem that we just discussed, namely, the difference between T-III's standards for interception of oral/wire communications, and those for electronic communications. The former are set forth in 18 USC 2516(1), the latter in 18 USC 2516(3).

For the purpose of this testimony, the two main differences are:
(1) that applications under 2516(3) do not require senior level DOJ approval and (2) that they are not limited to "certain federal felonies. Thus if we strike the sentence at the bottom of page two/top of page three (referring to authorization by a senior official of DOJ) and the last sentence in the first paragraph of page three ("Further, interception of communications is limited to certain specified felony offenses.") we will remove some of the misleading inferences as to which provision we follow when seeking court approval to intercept e-mail. There may may be other instances where the testimony suggests that we use 2616(1) rather than 2516(3); OGC should scrub the testimony again to check for such instances.

[redacted]

b6-1
b7c-1

CC: [redacted] CHARLES STEELE, [redacted] b6-1
b7c-1

Doc. #16

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

25 Pages were not considered for release as they are duplicative of DOCUMENT #13, OGC FRONT OFFICE FILE (PGS 20-44)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #17 (Pages 420-444)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

5/24/02 Release - Page 445

Doc. #18

IP Addresses

Example: 192.16.201.10

(Like a phone number)

Identifies a specific computer

How is Data Sent?

Example Email:

To: Jdoe@erols.com
From: JaneD@freedomnet.com
Subject: Blah

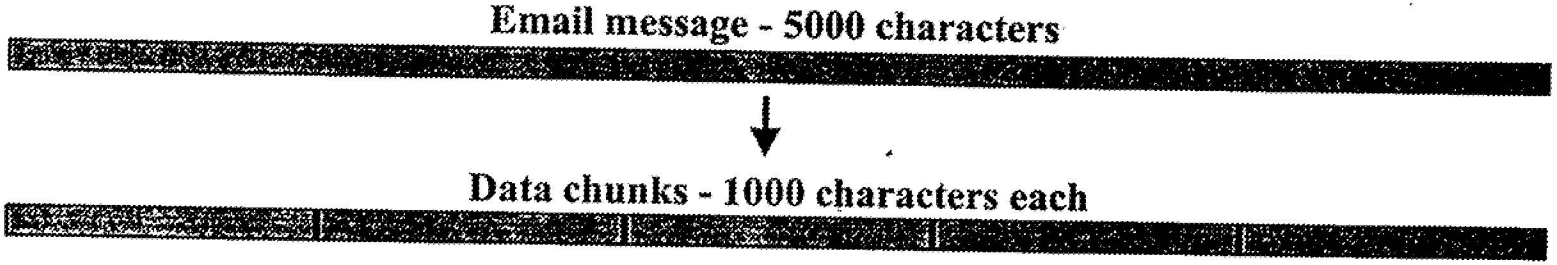
Hey John,

Blah blah blah

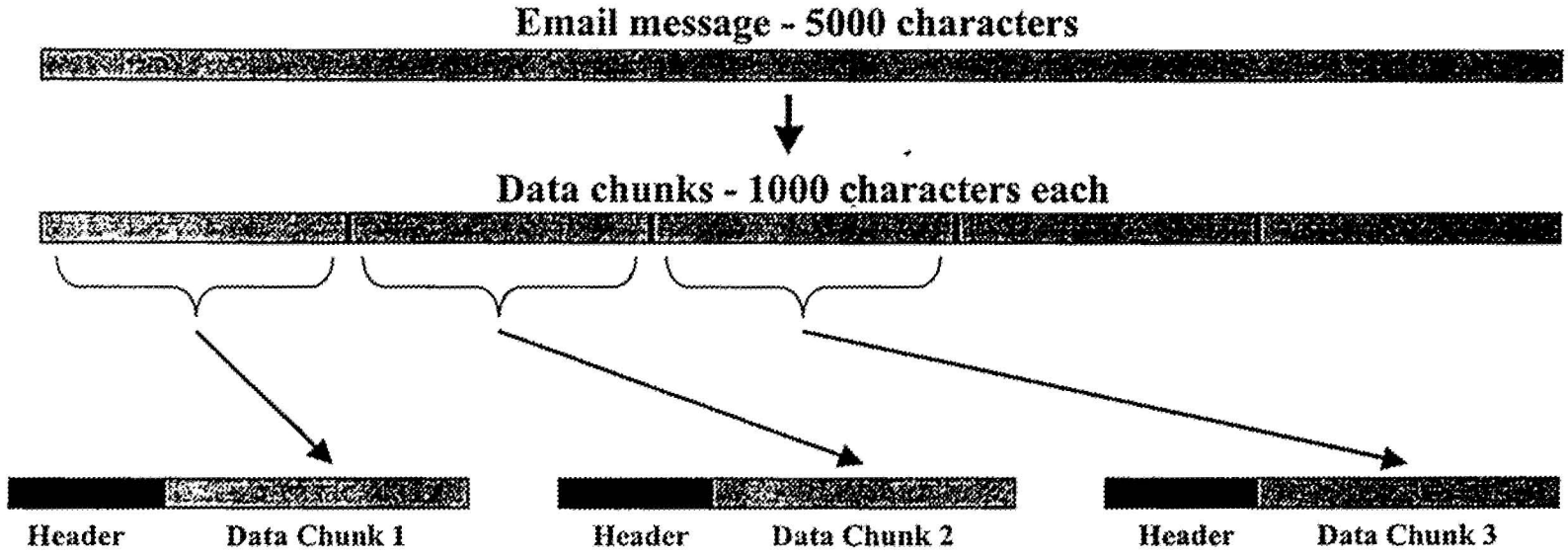
How is Data Sent?

Email message - 5000 characters

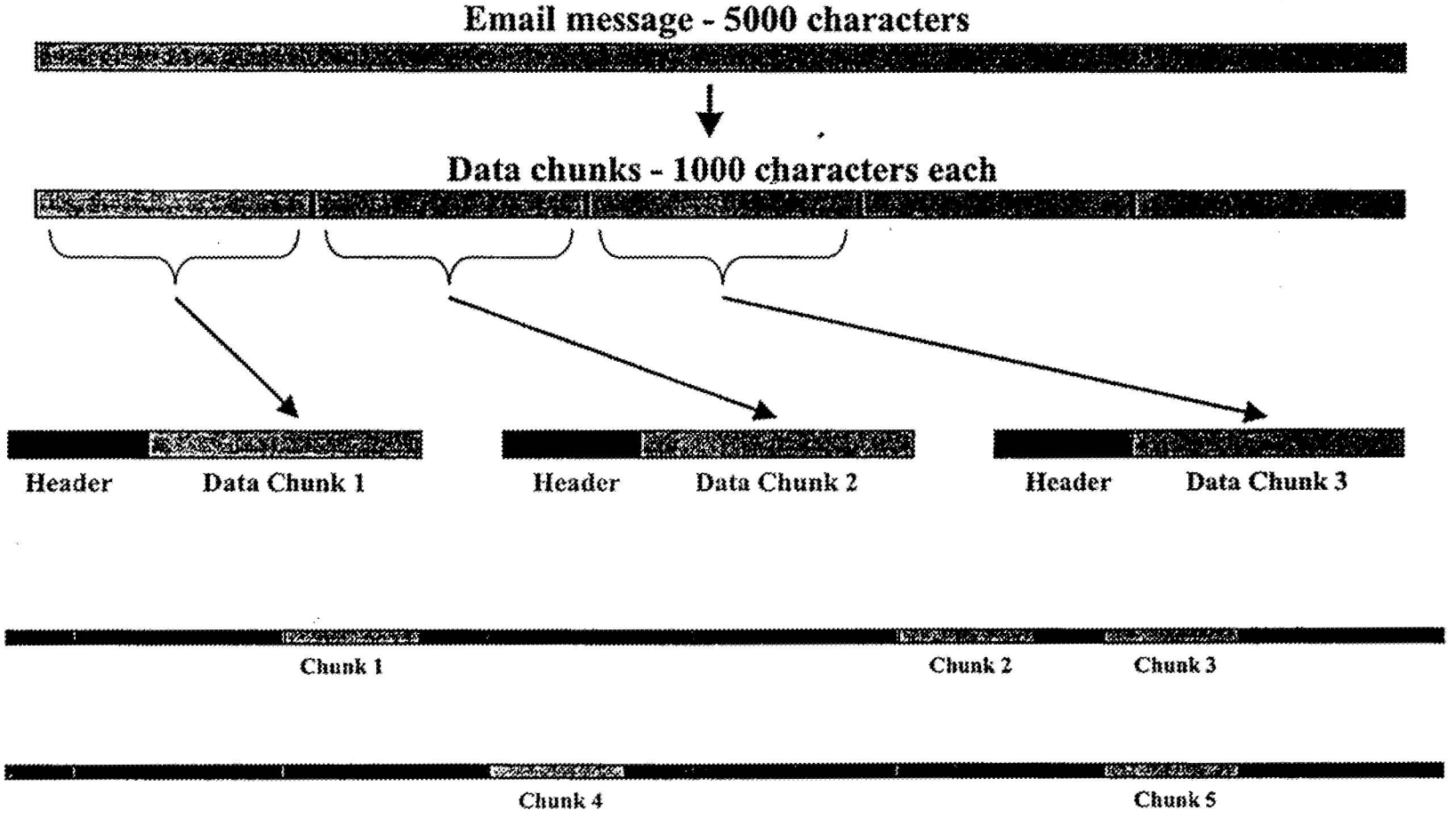
How is Data Sent?



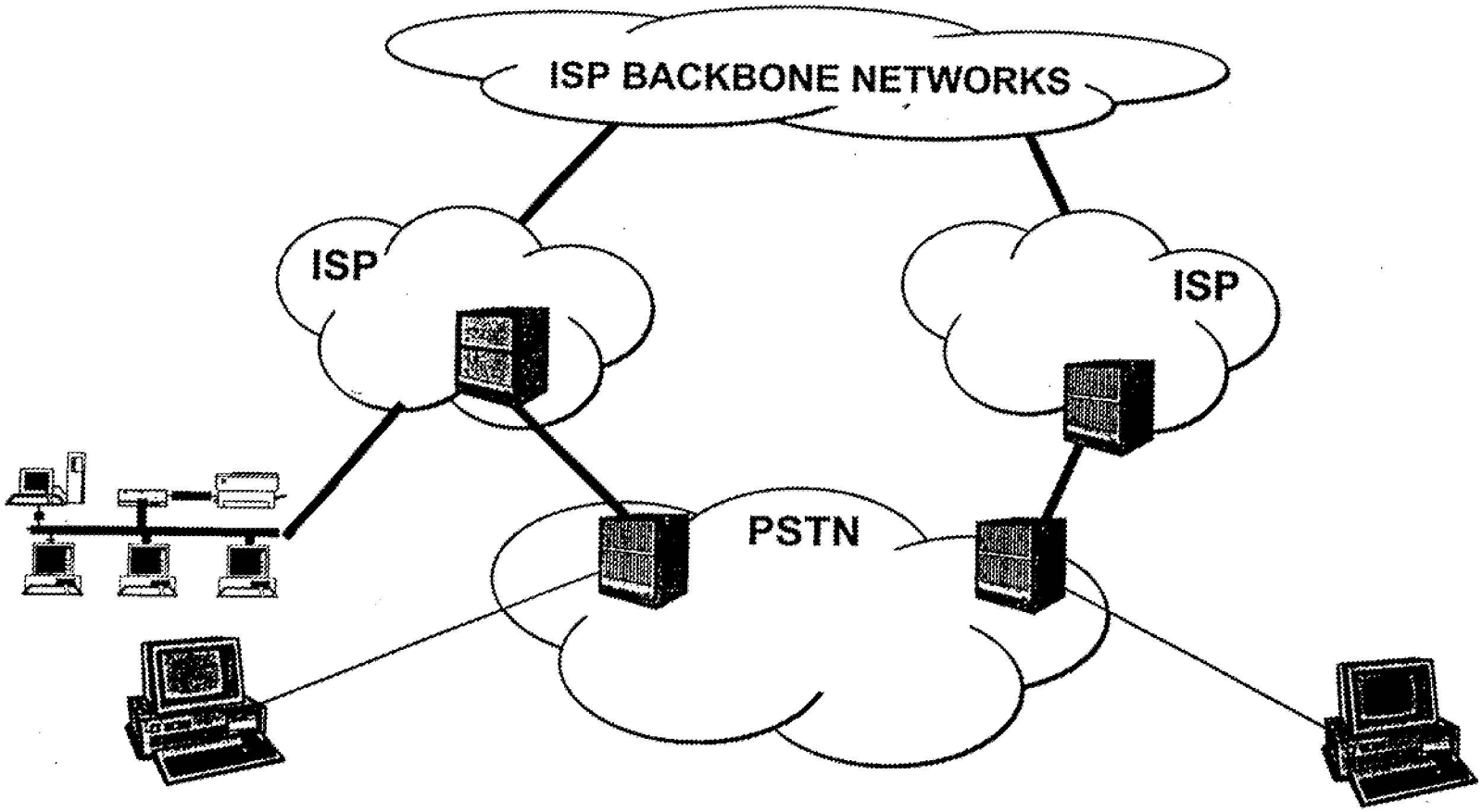
How is Data Sent?

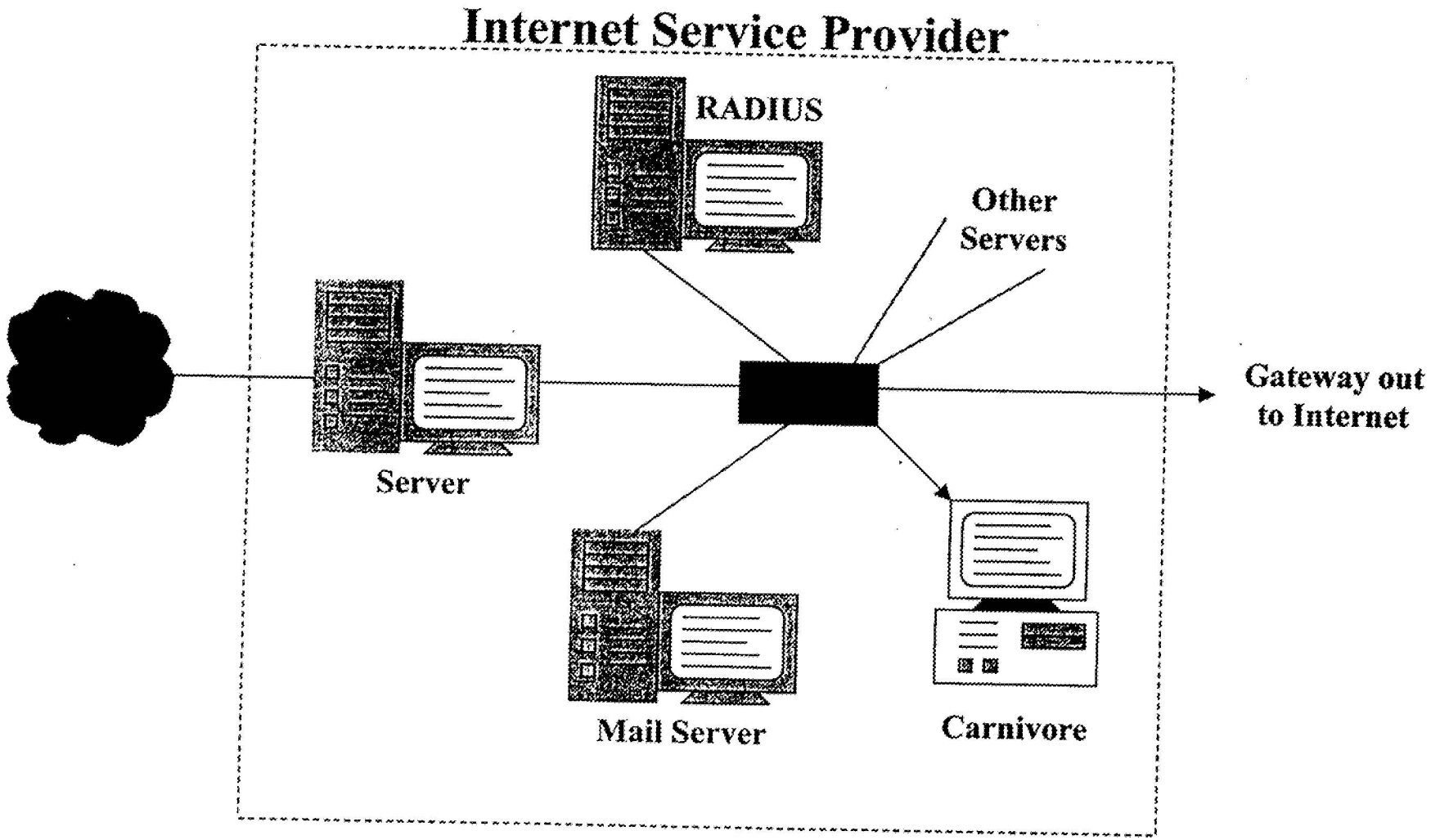


How is Data Sent?



Network Schematic




Internet Service Provider
RADIUS
Other Servers
Server
Gateway out to Internet
Mail Server
Carnivore

66-1/67C-1

66-1
67C-1

From: [redacted] 66-1 67C-1
To: LARRY PARKINSON
Subject: Carnivore

x [redacted] (703) [redacted]

66-1
67C-1

Larry: I wanted to bring you up to date re: Carnivore. I am leaving for Denver this morning to attend a Health Care Fraud Conference. I have brought [redacted] up to speed and he will be assiting you, OPCA and the Lab this week. There is one briefing scehdule with the Intelligence Committee on Wednesday, 7/19 at 10:00am. [redacted] will be going with [redacted] (OPCA) and [redacted] I was advised that next week there will be House hearings and that Dr. Kerr and you will be testifying. How [redacted] explained it to me was Dr.Kerr will read an opening statement that will incorporate both the technical aspects of Carnivore and the legal authority for its use. If this meets with your approval, both [redacted] and [redacted] will write the statement.

Carnivore is a sotware package that can be installed in box that can easily blend with other devices located at an ISP. It is only used under court order; it is not a continous running system. The software is maintianed at Quantico and is sent to a field office when needed. It was developed by us because we were not able to diferentiate between customers and/or messages. Jugdes were authorizing very narrow intercepts and we needed the ability to narrow our interception up front rather that with post-minimization. Carnivore "sniffs" up front and captures only those e-mails we are authorized to intercept or wnat to intercept.

How does it do this? It does this though a series of filters. The filters allow you to exclude those e-mails you do not want. As an example - the subject of your case is represented by counsel and communictes with him via e-mail. You can program Carnivore so that you will not capture these e-mails. Or you wnat to capture someone'e Web mail but not all his Web traffic (i.e. his brousing through catalogues shopping). Carnivore can limit the intercepts just to web mail. Therefore, it is actaully a privacy protector not invador.

Data is not stored on the Canivore device. It is stored on a disc or zip-drve that is locked by key by the agent and removed only by the agent so as to maintian chain of custody. The disc is then brought back to the field office and placed into a reading device. There is an additional minimization step that occurs at the field office to ensure that the case agent does not read any e-mails that he is not authorize to use pursuant to the court order. We may have information up front that allows us to filter e-mails but there may be times that we determine throught the course of the intercept that there are e-mails we can't have. Since most of our Carnivore intercepts are not real time, we need to post minimize. Once we learn that there is e-mail traffic we do not want, we can go back to the device and add filters to the program so that we will not capture the e-mails again.

I attended two briefings last week. One was with the Judiciary Committee minority staffers. They seemed more interested in understanding how Carnivore works, how long we have been using it, for what types of cases and were quite content once they learned that we only use Carnivore pursuant to a court order. They seemed quite satisfied with the briefing.

CC: CHARLES STEELE, [redacted] 66-1 67C-1

"Shall" to "may"

IP ADDRESS / series of phone #s

Signaling

clearer language -

nationwide subpoena for Reg order

Doc #19

WALL STREET JOURNAL

DATE 7/11/00
PAGE A3

FBI's Wiretaps To Scan E-Mail Spark Concern

By Neil King Jr.
And Ted Bridis
Staff Reporters of The Wall Street Journal

WASHINGTON—The Federal Bureau of Investigation is using a superfast system called Carnivore to covertly search e-mails for messages from criminal suspects.

Essentially a personal computer stuffed with specialized software, Carnivore represents a new twist in the federal government's fight to sustain its snooping powers in the Internet age. But in employing the system, which can scan millions of e-mails a second, the FBI has upset privacy advocates and some in the computer industry. Experts say the system opens a thicket of unresolved legal issues and privacy concerns.

The FBI developed the Internet wiretapping system at a special agency lab at Quantico, Va., and dubbed it Carnivore for its ability to get to "the meat" of what would otherwise be an enormous quantity of data. FBI technicians unveiled the system to a roomful of astonished industry specialists here two weeks ago in order to steer efforts to develop standardized ways of complying with federal wiretaps. Federal investigators say they have used Carnivore in fewer than 100 criminal cases since its launch early last year.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks. That would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing.

The system also troubles some Internet service providers, who are loath to see outside software plugged into their systems. In many cases, the FBI keeps the secret Carnivore computer system in a locked cage on the provider's premises, with agents making daily visits to retrieve the data captured from the provider's network. But legal challenges to the use of Carnivore are few, and judges' rulings remain sealed because of the secretive nature of the investigations.

Internet wiretaps are conducted only under state or federal judicial order, and occur relatively infrequently. The huge majority of wiretaps continue to be the traditional telephone variety, though U.S. officials say the use of Internet eavesdropping is growing as everyone from drug dealers to potential terrorists begins to conduct business over the Web.

SUBJECT: The FBI's e-mail tapping system, Carnivore.
TO: The computer industry
FROM: The FBI

1. The FBI installs one of its off-the-shelf PCs at the Internet service provider of the surveillance target.
2. The PC checks e-mails passing through the ISP for information that indicates whether an e-mail is going to or from the target.
3. If it is, the PC copies the full text of the e-mail to the PC's removable hard drive, which an FBI agent collects daily.
4. While it does analyze the destination and sender of other e-mails, Carnivore does not retrieve their full text.
5. Once the surveillance ends (average 45 days), an FBI agent gathers the computer from the ISP.

The FBI defends Carnivore as more precise than Internet wiretap methods used in the past. The bureau says the system allows investigators to tailor an intercept operation so they can pluck only the digital traffic of one person from among the stream of millions of other messages. An earlier version, aptly code-named Omnivore, could suck in as much as to six gigabytes of data every hour, but in a less discriminating fashion.

Still, critics contend that Carnivore is open to abuse.

Mark Rasch, a former federal computer-crimes prosecutor, said the nature of the surveillance by Carnivore raises important privacy questions, since it analyzes part of every snippet of data traffic that flows past, if only to determine whether to record it for police.

"It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring," Mr. Rasch said. "You develop a tremendous amount of information."

Others say the technology dramatizes how far the nation's laws are lagging behind the technological revolution. "This is a clever way to use old telephone-era statutes to meet new challenges, but clearly there is too much latitude in the current law," said Stewart Baker, a lawyer specializing in telecommunications and Internet regulatory matters.

Robert Corn-Revere, of the Hogan & Hartson law firm here, represented an unidentified Internet service provider in one of the few legal fights against Carnivore. He said his client worried that the FBI would have access to all the e-mail traffic on its system, raising dire privacy and security concerns. A federal magistrate ruled against the company early this year, leaving it no option but to allow the FBI access to its system.

"This is an area in desperate need of clarification from Congress," said Mr. Corn-Revere.

"Once the software is applied to the ISP, there's no check on the system," said Rep. Bob Barr, R-Ga., who sits on a House Judiciary subcommittee for constitutional affairs. "If there's one word I would use to describe this, it would be 'frightening.'"

Marcus Thomas, chief of the FBI's Cyber Technology Section at Quantico, said Carnivore represents the bureau's effort to keep abreast of rapid changes in Internet communications while still meeting the rigid demands of federal wiretapping statutes. "This is just a very specialized sniffer," he said.

He also noted that criminal and civil penalties prohibit the bureau from placing unauthorized wiretaps, and any information gleaned in those types of criminal cases would be thrown out of court. Typical Internet wiretaps last around 45 days, after which the FBI removes the equipment. Mr. Thomas said the bureau usually has as many as 20 Carnivore systems on hand, "just in case."

FBI experts acknowledge that Carnivore's monitoring can be stymied with computer data such as e-mail that is scrambled using powerful encryption technology. Those messages still can be captured, but law officers trying to read the contents are "at the mercy of how well it was encrypted," Mr. Thomas said.

Most of the criminal cases where the FBI used Carnivore in the past 18 months focused on what the bureau calls "infrastructure protection," or the hunt for hackers, though it also was used in counterterrorism and some drug-trafficking cases.

DOC. #20

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS (THROUGH 7/28/00)

PAGES REVIEWED: 49

PAGES RELEASED: 49

EXEMPTIONS CITED: NONE

NOTE: 57 pages from this file are duplicates to pages from The Office of General Counsel's Front Office file, The Office of General Counsel's/Technology Law Unit (TLU) file and The Office of General Counsel's/ Investigative Law Unit (ILU) file.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of DOC #20, OGC/INVESTIGATIVE LAW UNIT FILE pg. 453

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #1 (Page 456)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of Doc #1, OGC/TECHNOLOGY LAW UNIT FILE (PAGES 155-157)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages: DOCUMENT #2 (Pages 457-459)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Want to send this story to another AOL member? Click on the heart at the top of this window.

FBI e-mail Snooping Device Attacked

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - Civil liberties and privacy groups are railing against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.

The system, called ``Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.

When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.

Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

``Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target,'' read the letter. ``This 'trust us, we are the government' approach is the antithesis of the procedures required under our wiretapping laws.''

Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping data-tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, are already intrusive.

``Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target,'' Steinhardt said in an interview. ``When conducting these kinds of investigations, the information should be restricted to only addressing information.''

A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the House Judiciary subcommittee on the Constitution, said the congressman had no comment on the letter.

In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law firm in Washington, said he represented an Internet provider that refused to install the Carnivore system. The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared suits from customers unhappy with the government looking into all the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents,'' Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost its court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said the main problem with Carnivore is its mystery.

``The FBI is placing a black box inside the computer network of an ISP,'' Dempsey said. ``Not even the ISP knows exactly what that gizmo is doing.''

But Dempsey said Internet providers contributed to the problem, by saying that current technology does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

"The service providers said they didn't know how to comply with court orders," Dempsey said. "By taking that position, they have hurt themselves, putting themselves into a box."

Marcus Thomas, who heads the FBI's cybertechnology section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

"This is just a specialized sniffer," Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, and it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely - show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

"The FBI should make this gizmo an open-source product," he said. "Then the secret is gone."

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

American Civil Liberties Union: http://www.aclu.org

Center for Democracy and Technology: http://www.cdt.org

Pretty Good Privacy (PGP): www.pgp.com

AP-NY-07-12-00 0812EDT

Copyright 2000 The Associated Press. The information contained in the AP news report may not be published, broadcast, rewritten or otherwise distributed without the prior written authority of The Associated Press. All active hyperlinks have been inserted by AOL.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc #2, OGC FRONT OFFICE FILE (PAGE 2)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #4 (Page 462)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc #3, OGC/TECH. LAW UNIT FILE (PGS. 160-161)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #5 (Pages 463-464)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #2, OGC/TECH. LAW UNIT FILE (PAGES 158-159)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #C (Pages 465-466)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Tuesday July 18 07:02 PM EDT

Lawmakers: Stop Snooping on E-mail

WASHINGTON (APBnews.com) -- The pressure is mounting on the Justice Department to suspend a controversial new FBI wiretap system that allows agents access to vast amounts of e-mail traffic.

The so-called Carnivore system, which has come under fire from lawmakers as well as civil liberties groups since revelations about its existence surfaced last week, gives the FBI widespread access to monitor Internet service providers.

Members of Congress, led by House Majority leader Dick Armey, R-Texas, are drafting a letter they expect to send to Attorney General Janet Reno later this week urging her to put the wiretap system on hold until privacy concerns are resolved.

"The Carnivore system should not be used until concerns are addressed," Armey spokesman Richard Diamond told APBnews.com today. "There has been such a dramatic shift in what the FBI can monitor; there needs to be a public discussion. That's why the outrage. This was going on for a year and nobody knew."

Reno ordered review

Responding to concerns raised last week, Reno ordered a review of Carnivore but has no plans to order the program suspended, officials said today.

"The attorney general is looking into it to make sure she understands it and that it is applied fairly," said spokeswoman Chris Watney.

Last week Armey asked Reno and FBI Director Louis Freeh to "stop using this cybersnooping system until Fourth Amendment concerns are adequately addressed."

'The keys to the kingdom'

Rep. Bob Barr -- who described the Carnivore system surveillance abilities as "frightening" -- may demand similar restraints at a congressional oversight hearing on the program next Monday, a spokesman said.

"He is concerned about the lack of controls," said Brad Alexander, a spokesman for the Georgia Republican.

Civil libertarians, also outraged at the extent of the FBI's ability to monitor the e-mails of

Doc. #7

innocent people, also want Carnivore suspended.

"They want the keys to the kingdom," said American Civil Liberties Union Associate Director Barry Steinhardt, who is scheduled to testify at the subcommittee hearing Monday. "They want the entire stream of communications, and they expect us to trust them. Well, I don't. They have a history of abuse and stretching beyond the limits of what they are entitled to."

A critical tool, FBI says

FBI officials said they want the opportunity to demonstrate how critical the system is to its crime-fighting efforts.

"People need to know how critical this is," said bureau spokesman Paul Bresson, who said the agency wants to show the public how Carnivore works on Monday. "It gives us the ability to intercept conversations of criminals who are using the cyberworld the same way the rest of us are."

The FBI, in a statement describing Carnivore, said the system gives agents the "surgical" ability to intercept and collect information under legal orders.

Federal wiretaps have led to the convictions of 25,600 felons in the last 13 years, according to the FBI.

New wiretap rules sought

The renewed outcry comes a day after White House Chief of Staff John Podesta announced proposals that would require a more stringent approval process for FBI wiretaps, while at the same time expanding the agency's ability to conduct electronic surveillance.

The ACLU said the White House did not go far enough in its response to increasing government surveillance powers.

Steinhardt called the proposal a "camouflage for Carnivore," he said, when the administration should have "disavowed or suspended" the program. He also said the proposals stand little chance of being enacted before the Clinton administration leaves office.

The ACLU on Friday filed a Freedom of Information Act request for the source code, or computer program instructions, and other technical details about the Internet wiretapping program. The FBI said it will comply with FOIA rules and release whatever information it is able to

disclose by early August.

By Amy Worden, an APBnews.com staff writer.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #8, OGC FRONT OFFICE FILE (PAGES 8+9)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #8 (Pages 470-471)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc. #4, OGC FRONT OFFICE FILE (PAGE 4)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #9 (Page 472)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

6 Pages were not considered for release as they are duplicative of DOC. #9, OGC FRONT OFFICE FILE (PAGES 10-15)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #10 (Pages 473 - 478)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

9 Pages were not considered for release as they are duplicative of Doc #18, OGC/INVESTIGATIVE LAW UNIT FILE (PAGES 445 - 453)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #11 (Pages 479 - 487)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #10, OGC FRONT OFFICE FILE (PAGES 16+17)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #12 (Pages 488-489)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

14 Pages were not considered for release as they are duplicative of DOC. #13, PGS. 1-14, OGC FRONT OFFICE FILE (PGS. 20-33)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #13 (pages 490-503)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

BOB BARR
7TH DISTRICT
GEORGIA
ASSISTANT MAJORITY WHIP
PHONE (202) 225-2931
FAX (202) 225-2944
INTERNET: http://www.house.gov/barr

CONGRESS OF THE UNITED STATES

1207 LONGWORTH HOUSE BUILDING
WASHINGTON, D.C. 20515-1007

COMMITTEES
JUDICIARY
BANKING AND FINANCIAL SERVICES
GOVERNMENT REFORM
Subcommittee on Criminal Justice, Drug Policy, and Human Resources
VICE CHAIRMAN

July 24, 2000

The Honorable Louis J. Freeh
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue NW
Washington, D.C. 20535-0001

IN RE: Request for Information Pertaining to Carnivore System.

Dear Director Freeh:

In light of the recent disclosure of the Bureau's use of Carnivore, and given the substantial public interest in this matter, I hereby ask to review **all** records concerning the Carnivore system.

Included in the records should be :

- A description of Carnivore's capability
- A history of Carnivore's development and use
- The number of cases in which Carnivore has been used, and the number of Internet Service Providers (ISP) that have had the system installed.
- An analyses of the legal issues the Bureau considered before deploying the system.

While I would welcome any explanatory information the Bureau is willing to provide in response to my inquiry, I am requesting the **original**, source documents themselves, and would like to receive them before August 7, 2000. Given the potential impact on the public of Carnivore, I would like to make the material I receive public, and would like the Bureau to authorize this public release.

Thank you for your cooperation. If you have any questions, please contact my Legislative Counsel, Keri Allin, at 202/225-2931. I look forward to reviewing the information.

DISTRICT OFFICES

CARROLLTON
207 NEWNAN STREET
SUITE A
CARROLLTON, GA 30117
(770) 836-1776
FAX (770) 838-0436

LAGRANGE
200 RIDLEY AVE
LAGRANGE, GA 30240
(706) 812-1776
FAX (706) 885-9019

MARIETTA
999 WHITLOCK AVE
SUITE 13
MARIETTA, GA 30064
(770) 429-1776
FAX (770) 795-9551

ROME
600 EAST 1ST STREET
ROME GA 30161
(706) 290-1776
FAX (706) 232 7864

DOC #14

With kind regards, I remain,

very truly yours,

BOB BARR
Member of Congress

BB:ka

cc: The Honorable Janet Reno
The Honorable Dennis Hastert
The Honorable Richard Armey
The Honorable Tom DeLay
The Honorable J.C. Watts
The Honorable Dan Burton
The Honorable Henry Hyde
The Honorable Charles Canady
The Honorable Bill McCollum

NEW YORK TIMES

DATE 7-23-00

PAGE WK. IN REVIEW

Learning to Live With Big Brother

By STEPHEN LABATON

WASHINGTON

IN 1928, the Supreme Court took up the case of Roy (Big Boy) Olmstead, a bootlegger whose phones had been tapped by federal agents without a warrant. The court ruled that evidence obtained in that way was legal, prompting a remarkable dissent by Judge Louis D. Brandeis.

"The progress of science in furnishing the government with the means of espionage is not likely to stop with wiretapping," Justice Brandeis wrote in a dissent that the court adopted as the law nearly 40 years later. "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."

Thanks to the ubiquity of e-mail and the ingenuity of the F.B.I., that day has arrived. Over the last couple of weeks it has been widely reported that the F.B.I. is now using a computer program called Carnivore, which, once installed on the network of an Internet service provider, can troll through millions of e-mail messages and hone in on the electronic correspondence of suspects.

So far, the F.B.I. has reported using the program fewer than 25 times since it was developed 18 months ago, but that number is expected to grow quickly, since the bureau expects it to become an indispensable law enforcement tool, particularly in international espionage and terrorism cases.

That's fine, say critics, but Carnivore is also capable of simultaneously monitoring the communications of people not suspected of a crime. That has caused civil liberties groups and privacy advocates to worry that the technology might be used to monitor unpopular groups or political enemies, and not just suspected criminals.

Last week, as lawmakers on Capitol Hill began voicing their concerns, the White House moved to calm the growing storm. John Podesta, the president's chief of staff, outlined legislative proposals that would set legal requirements for surveillance in cyberspace.

Everyone agrees that some kind of legislation is needed to make sense of the existing patchwork of laws and court cases on electronic surveillance. At present, for example, e-mail sent via cable modem is more strictly protected than any other communication form — even telephone conversations. While law enforcement requests for lists of telephone calls to or from a particular line must be granted without question by a federal court, [illegible]

The White House proposed replacing these illogical distinctions with a uniform, rational set of standards. Civil liberties and privacy groups support this idea in principle, but are highly critical of the administration for refusing to explain how broadly it intends to use Carnivore or to describe what safeguards are in place for preventing its abuse.

Law enforcement officials say that computer systems like Carnivore are necessary because e-mail is becoming more frequently used for communication among criminals. And the officials note that these cybermonitors can actually be set to record communications much more selectively than a phone tap.

Carnivore could, for instance, be programmed to pick up the e-mail from only one sender and a particular computer, while excluding such e-mail as messages to or from, say, the sender's lawyer or wife. Phone taps, on the other hand, pick up everything.

At a news briefing on Friday, top F.B.I. officials also announced plans to submit Carnivore to analysis by independent academics, and noted that the system kept a log of what it was asked to pick up, which could be used by a court to spot any violations.

In making their case, supporters of cybersurveillance say that the only way to track e-mail is by combing through all of the messages on a particular network, because e-mail consists of a series of digital packets that are broken apart at the sending end and transmitted along multiple electronic paths before being reconstituted by the recipient's computer.

Nonetheless, privacy groups and some Internet service providers, or I.S.P.'s, say there remains a less intrusive alternative. The providers, like AOL or the Microsoft Network, could be ordered by a court to turn over specific material, rather than give the F.B.I. unlimited access to a network. That is precisely how telephone companies are treated; they cooperate with warrants for wiretaps and lists of telephone numbers called from a particular phone.

"The real question is who should be in control," said James X. Dempsey, staff attorney for the Center for Democracy and Technology, a civil liberties group in Washington. "It upsets the balance among competing interests and privacy for law enforcement to, in essence, kick the companies out of the way, hook up a black box, and say, don't touch it."

Other experts said that it was time for a reappraisal of all the standards used by the government to eavesdrop, particularly as the world moves into an era of digital communications that can be more readily monitored by computers and more easily masked by encryption.

As even household appliances begin to be wired into the Internet and many of our most personal thoughts and associations are now shared with the computer, the issue has taken on a new imperative and is being debated on a global scale.

THE British government (whose house-to-house searches in the English colonies led to the Fourth Amendment prohibition against unreasonable searches) is near to adopting a law, the Regulation of Investigatory Powers Bill, or R.I.P., that would require Internet service companies to finance the permanent installation of a Carnivore-like system for government use.

A similar system is already in place in Russia, while in the Netherlands a debate is raging over whether the government should have the authority to tap into e-mail at all.

"This debate really cries out for a return to first principles," said Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology.

Among the most important of such principles, he said, is that the government should always use the least intrusive investigative techniques before taking the invasive step of trying to intercept telephone calls or e-mail messages.

"What is the solution?" he asked. "A lot of oversight, a lot of accountability and a great deal of concern about the potential surveillance capabilities of the electronic police state." [illegible]

5/24/02 Release - Page 506

Doc #15

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #18 OGC FRONT OFFICE FILE (PGS. 124-125)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #16 (Pages 507-508)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

Copyright 2000 The Baltimore Sun Company
THE BALTIMORE SUN

July 24, 2000, Monday ,FINAL

SECTION: TELEGRAPH ,1A

LENGTH: 1119 words

HEADLINE: FBI taps of e-mail provoke concerns
Privacy issues lead to House hearings on 'Carnivore' work
Name called 'unfortunate'

BYLINE: Del Quentin Wilber

SOURCE: SUN NATIONAL STAFF

BODY:

WASHINGTON -- To civil libertarians and Internet service providers, a device created by the FBI to snoop through e-mail messages is as ominous as its name: "Carnivore."

Attached to an ISP's server, the contraption sifts through countless e-mail messages and copies specific information for federal agents seeking suspected criminals, including terrorists and child pornographers.

But critics say that, in the process of sifting out communications from its targets, Carnivore is also capable of retrieving the private messages of innocent people.

"This is a very dangerous device," said Barry Steinhardt, associate director of the American Civil Liberties Union. "It's unprecedented. It's the first time law enforcement has carte blanche access to the entire service provider's network."

The controversy surrounding the device with the foreboding name has caught the attention of Republican lawmakers, and a House Judiciary subcommittee is scheduled to hold a hearing on the matter today. Opponents and authorities who support the use of Carnivore are scheduled to testify.

After the system was disclosed in recent news accounts, sparking criticism from privacy advocates, FBI officials met with lawmakers and reporters to try to show that Carnivore is not nearly as intrusive as some fear.

For one thing, FBI officials said, they need the device to combat crime and threats to national security. They describe Carnivore as a "surgical" tool that would protect ordinary people from unintended searches.

"There are filtering mechanisms built in that limit the amount of information viewable to the human eye," said Paul Bresson, a spokesman for the bureau. "It ensures that only the exact communications authorized by a court are what we intercept."

For decades, federal agents and local police have been wiretapping suspects' phones after obtaining permission from judges. But those wiretaps are limited to a specific suspect and do not comb through phone calls at random.

Carnivore works much differently, though authorities still must obtain permission from a judge to scour e-mail messages or discover which Web pages a suspect visits.

Once they have court approval, agents attach the Carnivore device -- an ordinary- looking desktop computer -- to the ISP's main computer, and Carnivore " passively" sniffs through streams of data, FBI officials said.

Carnivore does not read e-mail messages or their subject lines, officials said. Instead, it searches for computer codes that direct the message to and from the suspect. Nor can it scan e-mail messages for key words, like "drugs or bomb," an FBI official said.

In other words, authorities say, Carnivore acts like an FBI agent authorized to scan envelopes sent by mail. The agent seeks a particular suspect's addressing information and pulls aside any qualified envelope and opens it.

Last week, after an outcry from critics, the White House said it would propose legislation to, among other things, require agents to seek Justice Department clearance before asking judges to authorize the use of Carnivore in a specific case. Such rules already cover voice wiretaps.

But the proposal was dismissed by civil liberties groups, who said it did not go far enough in protecting electronic communication.

For their part, FBI officials say, the White House proposal is not necessary: They say they abide by the rules governing voice wiretaps to use Carnivore.

Despite the assurances of FBI officials, civil liberties groups and congressional Republicans say they are wary of the system.

"It has the capability of grabbing it all," said Richard Diamond, a spokesman for Rep. Dick Armey, the Texas Republican who is the House majority leader and a sharp critic of Carnivore. "It all depends on who pushes the button. Someone could push the wrong button and have access to all sorts of information."

FBI officials dispute that assertion, though they concede that Carnivore has sometimes captured e-mail messages and data that were not targeted in their searches. They say they sealed such information and did not read it.

Earlier this year, an ISP tried unsuccessfully to prevent FBI agents from installing Carnivore on its network. After a brief court fight, the company, Earthlink, yielded to FBI demands and helped install the device.

FBI officials say they don't mind simply asking ISPs to provide them with e-mail sent by criminal suspects if that is possible. But, in most cases, agents would rather use Carnivore because it helps maintain security for criminal evidence. And many smaller ISPs are not capable of creating programs to obtain the necessary data, FBI officials said.

Though most ISPs have complied with court orders to install Carnivore, one major provider said it would refuse.

"We're not going to stand for this," said William L. Schrader, chairman and chief executive officer of PSINet Inc. "It's insidious. If they were to ask us with a court order to violate the privacy of all our customers, we would take this to the Supreme Court."

Authorities say that more criminals, especially those involved in child pornography and fraud, are increasingly using the Internet and e-mail to commit crimes.

About three years ago, agents and federal prosecutors began asking for real-time access to e-mail and Web-site visits, FBI officials said. The agents said they were worried about not having reliable and up-to-date intelligence.

FBI technicians began developing Carnivore, which was used for the first time about 18 months ago, authorities said. FBI officials declined to disclose any information about Carnivore-related cases but said the system has been used fewer than 25 times.

FBI officials said the "unfortunate" choice of a name emerged during internal discussions of the program.

At first, technicians called it "Omnivore" because it ate everything in sight. But as the system became more refined, technicians felt it needed a better name and changed it to **Carnivore:** a meat-eater.

"We're looking at how we name a lot of projects right now," an FBI official said. "This has been sobering."

FBI agents noted that they don't need **Carnivore** to read most old e-mail messages stored on ISP servers; they can already do so with court approval.

They described the **Carnivore** system as a last-resort measure to capture real-time communications.

Authorities on technology and society say they are hardly surprised that the system has generated anxiety, because many people now send more personal information over e-mail than over the phone.

Corporate snooping of employee e-mail and the unauthorized sale of client information by e-retailers have unnerved many computer users.

LOAD-DATE: July 25, 2000

FOCUS™
Search: General News;Baltimore Sun and Carnivore

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

About LEXIS-NEXIS | Terms and Conditions | What's New
Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

/ Pages were not considered for release as they are duplicative of DOC. #15, OGC FRONT OFFICE FILE (PAGE 121)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #18 (Page 512)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc. #16, OGC FRONT OFFICE FILE (PAGE 122)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #19 (Page 513)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Congressional Statement
Federal Bureau of Investigation

July 24, 2000

Statement for the Record of
Donald M. Kerr, Assistant Director
Laboratory Division
Federal Bureau of Investigation

on
Internet and Data Interception Capabilities Developed by FBI

Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.

Carnivore Diagnostic Tool

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the Internet and data interception capabilities developed by the Federal Bureau of Investigation. The use of computers and the Internet is growing rapidly, paralleled by exploitation of computers, networks, and data bases to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial service companies systems and steal customer home addresses and credit card information; criminals use the Internet's inexpensive and easy communications to commit large scale fraud on victims all over the world; and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques designed to work with new evolving computers and network technologies. The systems employed must strike a reasonable balance between competing interests- the privacy interests of telecommunications users, the business interest of service providers, and the duty of government investigators to protect public safety. I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting our Carnivore system as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly--and in fact this was the reason we choose to share information about this capability with industry experts several weeks ago. It is critically important as technology, and particularly communications technology, a continues to evolve rapidly, that the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our intercept capabilities are used only after court approval and that they are directed at the most egregious violations of national security and public safety.

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), commonly

referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". Such federal government interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws apply the Fourth Amendment's dictates concerning reasonable searches and seizures , and include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects and with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III, applications for interception of wire and electronic communications require the authorization of a high-level Department of Justice (DOJ) official before the local United State Attorneys offices can make an application to a federal court. Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are viewed by federal district court judges. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the type of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence--not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are met. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently by the court as well. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extension, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, that includes notice of the order the dates during which the interceptions were carried out, and whether or not the communication were intercepted. Upon motion, the judge may also direct that portion of the contents of the intercepted communication be made available to affected person for their inspection.

Under Title III, any person who was a part to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the contents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was not lawfully intercepted, the order authorizing or approving the interception was insufficient on its face or the interception was not in conformance with the order.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may recover in a civil action damages, including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.

The technical assistance of service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This is increasingly the case with the advent of advanced communication services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders by specifying that a court order authorizing the interception of communication shall upon the request of the applicant, direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example, in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in many cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed order, in order to be successfully implemented, require more sophisticated techniques to ensure that only messages for which there is court authorization to intercept are, in fact, intercepted. The increased detail in court orders responds to two facts.

First, the complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media

like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has court authorization, to the exclusion of all others, very difficult. Court orders, therefore, increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected as a passive collection device and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact, raises the third issue - that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to successfully implement, and

comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using the Carnivore system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires that authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another key reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependent upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices, without lawful authorization from a court.

I look forward to working with the Subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank you.

| 2000 Congressional Statement | FBI Press Room | FBI Home Page |

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the Internet and data interception capabilities developed by the Federal Bureau of Investigation. The use of computers and the Internet is growing rapidly, paralleled by exploitation of computers, networks, and data bases to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial service companies systems and steal customer home addresses and credit card information; criminals use the Internet's inexpensive and easy communications to commit large scale fraud on victims all over the world; and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques designed to work with new evolving computers and network technologies. The systems employed must strike a reasonable balance between competing interests - the privacy interests of telecommunications users, the business interest of service providers, and the duty of government investigators to protect public safety. I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception.

5/24/02 Release - Page 19

DOC. #21

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting our Carnivore system as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly–and in fact this was the reason we choose to share information about this capability with industry experts several weeks ago. It is critically important as technology, and particularly communications technology, a continues to evolve rapidly, that the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our intercept capabilities are used only after court approval and that they are directed at the most egregious violations of national security and public safety.

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". Such federal government interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications

5/24/02 Release - Page 320

without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws apply the Fourth Amendment's dictates concerning reasonable searches and seizures, and include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects and with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III, applications for interception of wire and electronic communications require the authorization of a high-level Department of Justice (DOJ) official before the local United State Attorneys offices can make an application to a federal court. Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are veiwed by federal district court judges. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the type of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence–not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are met. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently by the court as well. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extension, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, that includes notice of the order the dates

during which the interceptions were carried out, and whetehr or not the communication were intercepted. Upon motion, the jusge may also direct that portion of the contents of the intercepted communication be made available to affected person for their inspection.

Under Title III, any person who was a part to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the contents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was not lawfully intercepted, the order authorizing or approving the interception was insufficient on its face or the interception was not in conformance with the order.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may recover in a civil action damages, including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.

The technical assistance of service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This is increasingly the case with the advent of advanced communication services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's

execution of electronic surveillance orders by specifying that a court order authorizing the interception of communication shall upon the request of the applicant, direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example, in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in many cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed order, in order to be successfully implemented, require more sophisticated techniques to ensure that only messages for which there is court authorization to intercept are, in fact, intercepted. The increased detail in court orders responds to two facts.

First, the complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has court authorization, to the exclusion of all others, very difficult. Court orders, therefore, increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

5/24/02 Release - Page 525

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow

5/24/02 Release - Page 516

full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected as a passive collection device and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact, raises the third issue - that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical

5/24/02 Release - Page 527

personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to successfully implement, and comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using the Carnivore system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires that authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another key reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependent upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so

5/24/02 Release - Page 528

without the continued cooperation of our industry partners and innovations such as the Carnivore software. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices, without lawful authorization from a court.

I look forward to working with the Subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank you.

5/24/02 Release - Page 529

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #18, OGC FRONT OFFICE FILE (PGS. 124+125)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #22 (Pages 530-531)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

WASHINGTON POST

DATE 7-24-02
PAGE A01

Today in Congress

SENATE

Meets at noon.
Committees:
Energy and Natural Resources—Noon. Conservation and Reinvestment Act. 366 Dirksen Senate Office Building.

HOUSE

Meets at 12:30 p.m.
Committees:
Judiciary—1 p.m. Constitution subc. Fourth Amendment issues raised by FBI's e-mail message-capturing software. 2141 Rayburn House Office Building.
Judiciary—4 p.m. Constitution subc. Constitutional amendment to make a person who has been a U.S. citizen for 20 years eligible for the office of president. 2141 RyOB.

— Reuters

Doc #24

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

__1__ Pages were not considered for release as they are duplicative of Doc. #17, OGC FRONT OFFICE FILE (PAGE 123)

_____ Page(s) withheld for the following reason(s): _____

_____

_____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #25 (Page 534)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #21, OGC FRONT OFFICE FILE (PGS. 128 + 129)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #26 (Pages 535-536)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

WASHINGTON POST

DATE 9-25-00
PAGE E1

FBI Makes Case For Net Wiretaps

'Carnivore' System Faces Fire on Hill

By John Schwartz
Washington Post Staff Writer



BY BAY ISSTIG—THE WASHINGTON POST

"Criminals use computers to send child pornography to each other," said FBI official Donald M. Kerr.

Federal law enforcement officials defended "Carnivore"—the FBI's controversial Internet wiretap system—through more than two acrimonious hours of grilling by Democratic and Republican lawmakers yesterday, painting a chilling picture of an Internet that would become a safe haven for crooks and terrorists without proper surveillance.

"Criminals use computers to send child pornography to each other using anonymous, encrypted communications," FBI Assistant Director Donald M. Kerr told the House Judiciary subcommittee on the Constitution. "Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet."

Many of the lawmakers seemed just as concerned with the actions of the law enforcement officials. "The potential for abuse here is tremendous," said Rep. Spencer Bachus (R-Ala.). "What you're saying is 'Trust us.'"

Carnivore is a modified version of a common network-maintenance program known as a "packet sniffer." Carnivore offers great specificity—the ability to quickly collect just the "to" and "from" information in e-mail messages, for example, and not online banking transactions. That gives law enforcement the equivalent of the telephone world's "pen register" and "trap and trace" data—the origin and destination of all calls related to the subject.

Civil liberties groups and Internet service providers say the system raises troubling questions about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, they note, the new technology also could scan private information about legal activities, taking in vast amounts of information from innocent people as well as the suspect.

The critics also note that past experience has shown that law enforcement has overstepped its wiretap authority numerous times in the past.

Barry Steinhardt, associate director of the American Civil Liberties Union, said in his testimony: "Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target."

Officials of Internet service providers who oppose the technology say they are wary of putting equipment designed by others on their networks. They want the FBI to publish information on the software used so that ISPs can be sure that it does what the agency says.

The law enforcement officials pledged to present the system to a neutral third party for review but said they cannot release so much information about the system that it will become a target for evasion and hacking.

They insisted the Carnivore system actually provides greater privacy than previous methods of gathering electronic information because it can fine-tune what the machine hands over to investigators.

The FBI's Kerr also argued that agents won't "risk their integrity, their jobs and their futures" by abusing the law.

The toughest questioning came from Reps. Jerrold Nadler (D-N.Y.) and Robert L. Barr Jr. (R-Ga.), two congressmen rarely on the same side of an issue. Nadler peppered the officials with a series of questions that underscored the point that Carnivore, under the laws that govern pen-register surveillance, could be used without the difficult showing of "probable cause" required in a telephone wiretap.

Barr cited the investigation of missing White House e-mail and scornfully said the Clinton administration asserts that "we don't even know how to keep track of our own e-mail" while "now we see a very sophisticated system for keeping track of other people's e-mails!"

After the hearing, House Majority Leader Richard K. Armey issued a statement saying members of both parties showed "strong concerns that the administration is infringing on Americans' basic constitutional protection against unwarranted search and seizure.

"Until these concerns are addressed," he concluded, "Carnivore should be shut down."

WALL STREET JOURNAL

DATE 1-25-00
PAGE A24

Congressional Panel Debates Carnivore As FBI Moves to Mollify Privacy Worries

By Ted Bridis
Staff Reporter of The Wall Street Journal

WASHINGTON – The Federal Bureau of Investigation defended its Carnivore Internet-surveillance software to a largely skeptical congressional oversight panel, telling lawmakers that the electronic eavesdropping system is used only when approved by a judge and needed to protect citizens from criminals and terrorists.

-- To appease critics, the FBI yesterday announced a new tamper-proof auditing mechanism for Carnivore that it said will allow federal judges and others to review during each investigation how the system covertly monitors a suspect's e-mail. And the FBI said it plans to show Carnivore's inner workings to an organization that it will select to prove that the system works only as described by the government.

Members of the House Judiciary Subcommittee on the Constitution pressed FBI and Justice Department officials yesterday to prove that only e-mail and other Internet communications from criminals are harvested by the Carnivore software, whose blueprints are closely guarded. Rep. Melvin Watt (D., N.C.) raised the specter of "Big Brotherism." Rep. Henry Hyde (R., Ill.), chairman of the full Judiciary Committee, told them, "You can understand the skittishness of some people whose concern is privacy. And when you see some of the things that have happened here in Washington, it gives one reason to wonder and to worry."

"The potential for abuse here is tremendous, don't you agree?" added Rep. Spencer Bachus (R., Ala.).

"Congressman, I guess I don't agree with that," replied FBI General Counsel Larry Parkinson. And Donald Kerr, head of the FBI laboratory where Carnivore was developed, added that the software's use is subject to vigorous internal reviews, and its misuse would be a felony. "We don't have the right or the ability to just go fishing," he said.

Rep. John Conyers (D., Mich.) said, "If I could be assured that everybody wouldn't do the wrong thing because there is a statute making it criminal, that would reduce a lot of our efforts." But after Mr. Kerr offered assurances that Carnivore captures only the information it is programmed to seek, Rep. Conyers replied, "I don't know that we have any way of verifying the technological response that you're giving me."

A computer loaded with Carnivore can be plugged into an Internet-service provider's network, allowing the software to monitor the routing information for billions of distinct Internet communications such as e-mails and to make copies of full messages sent by or received from the subject of an FBI criminal investigation. The FBI maintains that no record is kept of any unrelated messages sent by innocent customers of the same Internet provider. The FBI has used the system 16 times so far this year, in six criminal cases and 10 national-security investigations.

Critics complain that, since the government refuses to disclose the blueprints for how its software works, there is little assurance that the FBI snooping isn't broader. The American Civil Liberties Union's associate director, Barry Steinhardt, testified that the system is "roughly the equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers with the assurance that the FBI will record only conversations of the specific target."

The panel discussed opening Carnivore's blueprints for review, which the FBI adamantly opposes. Even then, said Rep. Jerrold Nadler (D., N.Y.), civilian experts could be guaranteed only that they were looking at the current version of Carnivore, which is continually being upgraded and modified. "It could change at any time. You can't trust a police agency forever," he said.

Mr. Kerr said disclosing the program's code will allow computer hackers to find ways to defeat the system, and he wondered how often the code would have to be opened for review. "We would have a problem with full open disclosure," Mr. Kerr said. "When is enough enough?"

WASHINGTON TIMES

DATE: 7-25-00
PAGE: A1

Lawmakers rip FBI e-mail tracker

By William Glanz
THE WASHINGTON TIMES

Federal law enforcement agents say they have used the controversial Carnivore software program to track e-mail of suspects 25 times in the past two years.

But agents have never used the program illegally or tracked e-mail they were not authorized to track by a court order, FBI Assistant Director Donald Kerr told the House Judiciary subcommittee on the Constitution yesterday.

Despite the restraint the FBI says it has used, privacy rights advocates criticized law enforcement agents for using Carnivore and lawmakers expressed skepticism about the federal government's use of the Internet surveillance tool.

House Majority Leader Dick Armey, Texas Republican, said yesterday Carnivore should be suspended until concerns of privacy advocates and needs of law enforcement are reconciled.

"Until these concerns are addressed, Carnivore should be shut down," he said.

Carnivore enables investigators to pick out specific e-mail messages traveling through an Internet service provider's computer system so it can monitor who a suspect contacts and who contacts a suspect.

Mr. Kerr and other federal officials said the high-tech surveillance system is crucial to help them keep up with an increasingly sophisticated breed of tech-savvy criminals and crucial to help them keep the Internet safe.

"Many of the crimes that we confront every day in the physical world are beginning to appear on line," said Deputy Assistant Attorney General Kevin DiGregory. "If we fail to make the Internet safe, public confidence in using the Internet and e-commerce will [illegible] endangering the very [illegible] by the information [illegible] Carnivore is simply an [illegible] that is used on [illegible] narrowly defined [illegible] and only when authorized by law to meet our responsibilities to the public," he [illegible]

Surveillance tool employed 25 times

But lawmakers expressed concern about a lack of checks and balances on law enforcement agents using Carnivore.

"The potential for abuse here is enormous," said Rep. Spencer Bachus, Alabama Republican.

FBI General Counsel Larry Parkinson said Carnivore is a little-used tool. When it is used, Mr. Kerr said, agents follow the law carefully, and if they are caught collecting more data than allowed, they can be imprisoned up to five years for committing a federal felony.

"In the past, we've had many agencies go beyond the scope of their authority," said Rep. John Conyers Jr., Michigan Democrat.

Mr. Kerr said the FBI and Department of Justice will seek an independent review of Carnivore this year to show they aren't misusing the program.

Lawmakers and privacy rights advocates also criticized federal officials for using Carnivore when Internet service providers could just as easily collect information being sought.

"There ought to be more control in the hands of the [Internet service providers]," said Alan Davidson, a lawyer with the District-based civil liberties group Center for Democracy and Technology.

Mr. Kerr argued that few of the nation's estimated 10,000 Internet service providers have the means to sift through e-mail traffic and collect them for law enforcement.

But Robert Corn-Revere, an attorney who represented Atlanta-based Internet service provider EarthLink, said EarthLink was gathering e-mail information at the federal government's request earlier this year when it was forced to comply with a court order and let federal officials install Carnivore on its computers.

The federal government was upset that EarthLink was capturing few e-mail messages, Mr. Corn-Revere said, and it needlessly installed Carnivore.

American Civil Liberties Union Associate Director Barry Steinhardt suggested Carnivore's source code be made public. The source code is the set of instructions a programmer writes, and it will show just what Carnivore is capable of retrieving. The ACLU has filed a Freedom of Information Act request with the FBI to get the source code.

Even though they had a raft of questions about Carnivore and its use, lawmakers yesterday didn't express any willingness to make immediate changes in the federal government's authority to use the surveillance program.

"We should be sensitive to any potential for abuse of the Carnivore system. Even a system designed with the best of intentions to legally carry out essential law enforcement functions may be a cause for concern if its use is not properly monitored," said Rep. Charles T. Canady, Florida Republican.

Doc 29

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

__1__ Pages were not considered for release as they are duplicative of Doc #20, OGC FRONT OFFICE FILE (PG. 127)

_____ Page(s) withheld for the following reason(s): _____

_____

_____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #30 (Page 540)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of DOC #19, OGC FRONT OFFICE FILE (PG. 126)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #31 (Page 541)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

AMERICAN CIVIL LIBERTIES UNION

Barry Steinhardt
Associate Director

National Headquarters 125 Broad Street, New York, NY 10004-2400
Tel (212) 549-2500 Fax (212) 549-2653

July 26, 2000

John Kelso Jr.
Federal Bureau of Investigation
Chief, FOI/PA Section, Rm. 6296 JEH
Washington, D.C. 20535-0001

Office of Public Affairs
United States Department of Justice
Room 1128
950 Pennsylvania Avenue NW
Washington DC 20530-0001

Attention:

We are writing pursuant to the Freedom of Information Act (5 U.S.C. § 552) to request expedited handling of our July 14, 2000 request for all agency records (including letters, correspondence, tape recordings, notes, data, memoranda, email, computer source and object code, technical manuals, technical specifications, or any other materials) held by the Federal Bureau of Investigation (FBI) regarding the following:

1. The computer system, software or device known as "Carnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers;

2. The computer system, software or device known as "Omnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers, and

3. The computer system, software or device known as "EtherPeek", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers.

We seek expedited review of this FOIA request because this information relates to impending policy decisions to which informed members of the public might contribute.

Nadine Strossen *President* Ira Glasser *Executive Director* Kenneth B. Clark *Chair, National Advisory Council* Richard Zacks *Treasurer*

Doc #32

Timely public access to these materials is necessary to fully inform the public about the issues surrounding communications interception and related technological developments.

Specifically, we request expedited access pursuant to 28 C.F.R. 16.5(d)(1)(ii), which allows such processing based on an "urgency to inform the public about an actual or alleged government activity, if made by a person primarily engaged in disseminating information." As explained earlier, the Federal government's use of Carnivore is a matter of great importance because it raises serious questions as to the government's willingness to protect individual privacy and civil liberties. Note that public interest about Carnivore has been so strong that Congress has seen fit to hold at least one hearing on this subject. (See *Oversight Hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program,"* 106th Cong. (2000).) A recent Congressional hearings and slew of press coverage indicate the "urgency to inform the public" on this issue. (See, e.g., John Schwartz, "Republicans Oppose FBI Scrutiny of E-Mail," Washington Post, July 21, 2000 at A1; D. Ian Hopper, "Eating Away at Privacy?" Associated Press, July 12, 2000; "Eyeing High-Tech Private Eyes," ABCNews.com, July 14, 2000; "FBI says Carnivore will not devour privacy," CNN.com, July 21, 2000; Margaret Johnston, "FBI Demos E-Mail 'Carnivore'," PC World.com, July 21, 2000.)

Moreover, the American Civil Liberties Foundation (ACLU Foundation) meets the criterion laid out in National Security Archive v. Department of Defense, where a representative of the news media is defined as an entity that "gathers information of potential interest to a segment of the public" and "uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." 881 F. 2d at 1387. The ACLU Foundation publishes newsletters, frequent press releases, news briefings, right to know handbooks, and other materials that are disseminated to the public. Its material is widely available to everyone including tax exempt organizations, not-for-profit groups, law students and faculty through its public education department. The ACLU Foundation disseminates information through publications available on-line at www.aclu.org as well. Thus the organization meets the pertinent regulatory requirements for expedited access.

In addition, we request expedited access pursuant to 28 C.F.R. 16.5(d)(1)(iv), which allows such access for a "matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence." Again, the recent Congressional hearings, as well as the storm of media coverage about Carnivore and related computer programs provide ample evidence of the "widespread and exceptional media interest" in this issue. Moreover, the revelations about Carnivore raise doubts as to the government's integrity in safeguarding the privacy of individuals.

We have enclosed certification (for the purposes of expedited access) with this letter.

If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the act. We expect you to release all segregable portions of otherwise exempt material. We reserve the right to appeal your decision to withhold any information or to deny a waiver of fees.

We look forward to your reply within ten calendar days, as required under 28 C.F.R. 16.5(d)(4).

Thank you for your assistance.

Sincerely,

Barry Steinhardt, Esq.
On behalf of the ACLU Foundation

Enclosures

CERTIFICATION

To whom it may concern:

I certify that the following facts are true and correct to the best of my knowledge and belief:

1. The American Civil Liberties Foundation (ACLU Foundation) meets the criterion laid out in National Security Archive v. Department of Defense, where a representative of the news media is defined as an entity that "gathers information of potential interest to a segment of the public" and "uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." 881 F. 2d at 1387. The ACLU Foundation publishes newsletters, frequent press releases, news briefings, right to know handbooks, and other materials that are disseminated to the public. Its material is widely available to everyone including tax exempt organizations, not-for-profit groups, law students and faculty for no cost or for a nominal fee through its public education department. The ACLU Foundation disseminates information through publications available on-line at www.aclu.org as well.

2. The disclosure of information regarding the following computer systems is in the public interest:

- The computer system, software or device known as "Carnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers;

- The computer system, software or device known as "Omnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers, and

- The computer system, software or device known as "EtherPeek", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers.

Records regarding Carnivore, Omnivore and EtherPeek are likely to contribute significantly to the public understanding of the activities of the government. The ACLU Foundation is a nonprofit 501(c)3 research and education organization working to increase citizen participation in governance issues. The ACLU Foundation is making this request specifically for the public's enhanced understanding of lawfully authorized wiretapping, its relationship to constitutional guarantees of privacy as well as an

understanding of global technological developments in wire and electronic networks that facilitate and expedite such wiretapping. The public's interest is particularly pertinent in light of advancing communications technology and the rapid growth of the World Wide Web. These developments have greatly increased the communications interconnectedness of all the countries in the world, especially technologically advanced nations like the US and the Netherlands.

3. The information requested regards a "matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence." Public interest in Carnivore has grown to such an extent that Congress has held at least one hearing on this subject. (See *Oversight Hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program,"* 106th Cong. (2000).) The tremendous amount of media coverage about Carnivore and related computer programs also provides strong evidence of the "widespread and exceptional media interest" in this issue. (See, e.g., John Schwartz, "Republicans Oppose FBI Scrutiny of E-Mail," Washington Post, July 21, 2000 at A1; D. Ian Hopper, "Eating Away at Privacy?" Associated Press, July 12, 2000; "Eyeing High-Tech Private Eyes," ABCNews.com, July 14, 2000; "FBI says Carnivore will not devour privacy," CNN.com, July 21, 2000; Margaret Johnston, "FBI Demos E-Mail 'Carnivore'," PC World.com, July 21, 2000.) In addition, the requested material may provide answers to serious questions regarding the government's willingness to protect individual privacy and civil liberties.



7/26/00

Barry Steinhardt, Esq.
On behalf of the ACLU Foundation

July 26, 2000

CARNIVORE

Diagnostic Tool

Internet and Data Interception Capabilities Developed by the FBI, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. donald M. Kerr

The Nation's communications networks are routinely used in the commission of serious criminal activities, including espionage. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities.

The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence -- not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,600 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques.

In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the

Stop Carnivore
July 27, 2000

news & info

Twenty-eight Members of Congress sent the following letter to Attorney General Janet Reno asking her to suspend operation of the Carnivore Internet surveillance system until the serious privacy issues involved have been addressed.

Congress of the United States

Washington, DC 20515

July 27, 2000

The Honorable Janet Reno, Attorney General
US Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Attorney General Reno,

We are writing to express our strong reservations about a new Internet monitoring system developed by the Federal Bureau of Investigation, called Carnivore.

Carnivore, it has been reported, enables the Federal Government to scan all of the traffic on an Internet Service Provider's network. Although national security and law enforcement are essential priorities, Carnivore has raised serious Fourth Amendment questions. Should the federal government be trusted with this kind of personal communication?

Consumer confidence in the privacy and security of the Internet are essential for continued growth of e-commerce. People should feel secure that the federal government is not reading their email, no matter how worthy the objective.

Given the uproar Carnivore has created, and the potential impact reports on Carnivore could have on consumer confidence in the Internet, we urge you to suspend any activity involving the development or use of Carnivore until the serious privacy issues involved have been satisfactorily answered.

Sincerely,

Dick Armey	Tom DeLay	J.C. Watts
Kevin Brady	John Thune	Larry Combest
Jack Metcalf	Brian Bilbray	Julia Carson
Charlie Norwood	Bob Barr	Bill Archer
Nancy Johnson	Jim McCrery	Terry Everett
Richard Pombo	John McHugh	Tom Campbell
Sonny Callahan	Jim Kolbe	Donald A. Manzullo
Tom Coburn	Richard Baker	Zach Wamp
Charles H. Taylor	Mac Thornberry	Jim Gibbons
Dan Miller		

Additional supporters:

Cynthia McKinney	Doc Hastings	Bob Goodlatte
Ron Paul		

Related Links
The e-Contract

Remarks on the e-Contract with High Tech America

WebVote: Internet Privacy

Stop Carnivore

More Questions About FBI Cybersnooping System

WebVote

Want to send this story to another AOL member? Click on the heart at the top of this window.

Reno describes FBI Internet-wiretap system review

WASHINGTON, July 27 (Reuters) - U.S. Attorney General Janet Reno described on Thursday a two-step process to review a new FBI Internet-wiretap system called Carnivore that has raised privacy concerns.

With lawmakers and privacy advocates concerned the system allows for widespread surveillance of e-mails, Reno said the first step will be for a group of academic experts to conduct a detailed review of the computer program's source code.

"Those experts will report their findings to a panel of interested parties, people from the telecommunications and computer industries, as well as privacy experts," Reno told her weekly Justice Department news briefing.

"I'm very anxious to get this review under way. The FBI is working on it, and representatives of the bureau are meeting with privacy advocates and representatives of the telecommunications and computer industry to pursue it and to develop a protocol for the review," she said.

The system allows the FBI to intercept the e-mails of a criminal suspect among the flood of other data passing through an Internet service provider.

FBI officials maintain the court-authorised wiretaps will only focus on criminal suspects who are targets of an investigation. But privacy advocates fear the system may cast too wide a net, encompassing private information about legal activities.

Reno said the two-step process was worked out with the FBI, and that she wanted the review to be done "as soon as possible."

She said the system would not be suspended until the review has been completed. "I think that we will continue to make sure that it is implemented carefully and there is no abuse in its use."

In a letter to Reno, 27 House of Representatives Republicans and one Democrat expressed "strong reservations" about the system and urged Reno to halt its operation "until the serious privacy issues have been satisfactorily answered."

The lawmakers added, "People should feel secure that the federal government is not reading their e-mail, no matter how worthy the objective."

Reno stopped short of agreeing to release the source code. The American Civil Liberties Union has asked for it to be made public so it could evaluate the software's true capabilities.

14:06 07-27-00

Copyright 2000 Reuters Limited. All rights reserved. Republication or redistribution of Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Reuters. Reuters shall not be liable for any errors or delays in the content, or for any actions taken in reliance thereon. All active hyperlinks have been inserted by AOL.

Want to send this story to another AOL member? Click on the heart at the top of this window.

Bill Addresses E-mail Surveillance

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - A move is under way in Congress to increase the burden on federal law enforcement agencies to justify monitoring people's e-mail messages and other communications.

Rep. Bob Barr confirmed that he and his staff are at work on a bill that would rein in the FBI's new ``Carnivore'' surveillance system and place additional restrictions on telephone wiretaps as well.

Barr, R-Ga., said he was concerned about computer eavesdropping capability before attending a hearing on Capitol Hill earlier this week, and he said he ``came out of it scared.''

Privacy advocates and computer experts called Carnivore a ``black box'' in testimony Monday, and said only the FBI knows what it truly does. They also contended that information the FBI gets from the device, installed at a suspect's Internet service provider, is far more than what could be gleaned from a telephone wiretap and statutes governing telephone surveillance are being misused.

In a telephone ``trap-and-trace'' or ``pen register'' wiretap, authorities can get a list of phone calls made to and from a certain telephone number. The usable information is limited to the 10-digit telephone numbers and the time of the call, and the phone company, when given a court order, provides the information.

Current laws and judicial precedent say that the numbers a person dials are not private communications, and therefore authorities do not need to show that a crime has been committed.

With Carnivore, that statute is being extended to the Internet world.

The details of Barr's bill aren't clear yet, but he said it would address the issue of translating telephone wiretap law to the Internet by designing strict constraints for monitoring the medium. It would also make sure that evidence gained from an e-mail tap would not yield more information than a similar court order for a telephone tap.

The FBI's new surveillance mechanism sits at the subject's ISP and scans the addressing information coming from or going to the suspect's computer. This can reveal far more information than a simple e-mail address, such as a subject line describing the contents of the message.

``Capturing Internet origin and destination address instead of 'numbers dialed' could create a much more intrusive form of surveillance that is not clearly supported by law,'' said Alan B. Davidson, staff counsel at the Center for Democracy and Technology.

For authorities to be able to request e-mail contents they must show probable cause and obtain a search warrant. The same is true for listening in on a telephone call.

Regarding the inner workings of Carnivore, the FBI is resisting a Freedom of Information Act request by the American Civil Liberties Union for Carnivore's computer code, but said it will submit to an external review.

Since the Carnivore computer, devoid of keyboard and mouse, sits at the suspect's ISP and is locked down from any manipulation from non-FBI personnel, Internet providers have bristled at the idea of letting it sit on their networks.

Donald M. Kerr, assistant director of the bureau's laboratory division, said in an interview that the FBI would love to have the ISP provide the information authorities need, but the cost and technical knowledge can be prohibitive for small Internet companies.

Peter William Sachs, a lawyer and president of ICONN, a small Internet provider in Connecticut, said the job could be done with two lines of computer code, and called it a ``trivial'' task.

Barr concurred, saying "I'm not satisfied with the FBI's explanation."

But he will have a stiff challenge in keeping apace of the changes in technology.

Not only can Carnivore monitor e-mails, Kerr said, but it also can monitor Web browsing, chat rooms and all sorts of other communications.

However, it is the FBI's argument that although Carnivore can read those things, it's a difference between "capability and authorization," Kerr said.

"People seem to conjure up this vision that FBI personnel are unsupervised and unconstrained in the use of these tools," he said. "To misuse these authorities and to go outside the scope of the court order is to commit a federal felony. It's, to me, not conceivable that groups of our employees would run that kind of risk in doing their job."

Kerr again noted a separate audit trail maintained by Carnivore that keeps track of its activity and configuration, and said that trail is an extra safeguard against misuse.

Barr said he expects resistance from other legislators, even from other Republicans, but said he will not let the FBI go unchecked.

"They want to just go out and rely on scaring people to death, that if they don't get this authority, the terrorists will take over the country, and say 'we're out to save the world,' " Barr said.

AP-NY-07-27-00 0904EDT

Copyright 2000 The Associated Press. The information contained in the AP news report may not be published, broadcast, rewritten or otherwise distributed without the prior written authority of The Associated Press. All active hyperlinks have been inserted by AOL.

7/27/00


YES. WE SPY ON YOUR E-MAIL, BUT IT'S FOR YOUR OWN SAFETY. YOU CAN TRUST US WITH YOUR PERSONAL INFORMATION.
FBI
BY THE WAY... ...YOUR SON IS GAY, YOUR DAUGHTER'S PREGNANT AND YOUR AUNT IDA'S SHINGLES ARE FLARING UP AGAIN!
FBI
THE FREE LANCE-STAR

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of DOC. #24, OGC FRONT OFFICE FILE (PG. 151)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #37 (Page 555)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

__1__ Pages were not considered for release as they are duplicative of DOC. #26, OGC FRONT OFFICE FILE (PG. 153)

_____ Page(s) withheld for the following reason(s): _____

_____

_____

X The following number is to be used for reference regarding these pages:
DOCUMENT #38 (Page 556)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Representing Florida's 12th District
Charles T. Canady
Chairman, House Judiciary Subcommittee on the Constitution
2432 Rayburn House Office Building • Washington, D.C. 20515 • 202-225-1252

For Immediate Release
July 27, 2000

Contact: Michelle Morgan Knott
(202) 225-1252

Rep. Canady Introduces Bill to Update Wiretap Laws

E-Mails and Stored Internet Communications Would Be Covered

WASHINGTON, D.C. — **Rep. Charles T. Canady** (R-FL), Chairman of the House Judiciary Subcommittee on the Constitution, today introduced the Electronic Communications Privacy Act of 2000. The bill would update the federal wiretap laws to cover e-mail and stored electronic communications, as well as provide special requirements for government tracing of e-mail addresses. Canady is joined by original cosponsor Rep. Asa Hutchinson (R-AR).

> **"This legislation helps move our federal wiretap laws into the 21st Century," Canady said. "We have entered a new age with the Internet, and we need a new law to reflect the rapid changes in technology. While this legislation does not answer all the difficult issues raised by recent technological advances, it does provide for some reasonable reforms that will protect the privacy rights of Americans."**

Earlier this week, Rep. Canady chaired a Constitution Subcommittee hearing on Fourth Amendment issues raised by the FBI's "Carnivore" program. The FBI designed and developed Carnivore to isolate, intercept and collect communications that are the subject of lawful court orders. The July 24th hearing featured witnesses from law enforcement, civil liberty organizations, privacy organizations and representatives from the business community.

BILL SUMMARY

The Electronic Communications Privacy Act of 2000 has three sections. The first section amends the "statutory exclusionary rule" to also exclude from use as evidence illegally intercepted "electronic communications" and illegally obtained "stored electronic communications." The bill simply adds electronic communications to the previously covered wire and oral communications.

The second section of the bill requires the federal government to produce annual reports regarding its requests for orders for the disclosure of "stored electronic communications." This reflects virtually identical disclosure requirements the federal government must meet regarding the use of electronic wiretaps.

The final section of the legislation amends the definition of "pen register" and "trap and trace" devices, defining them to allow the identification of an "e-mail address." In addition, the section requires that, if a pen register or trap and trace device is used to identify an e-mail address, the

-more-

federal government must first demonstrate to a court that "specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use [of a pen register or trap and trace device] is relevant to an investigation of that crime."

For a copy of Rep. Canady's legislation (7 pages) please call Michelle Knott at (202) 225-1252.

###

OMAHA DAILY HERALD FOUNDED [illegible]
OMAHA DAILY WORLD FOUNDED BY GILBERT M. HITCHCOCK 1885
OMAHA WORLD-HERALD FIRST PUBLISHED JULY 16, 1889

Omaha World-Herald

JOHN GOTTSCHALK, *Publisher*
LAWRENCE D. KING, *Executive Editor* FRANCIS L. PARTSCH, *Editorial Pages Editor*
DEANNA J. SANDS, *Managing Editor*

Is Carnivore on a Leash?

The FBI insists that its recently disclosed "Carnivore" Internet surveillance system is not a wide-spectrum threat to privacy. Federal operatives say that in fact it is used only pursuant to normal Justice Department procedures. In many or most instances these rest on a judge-signed surveillance order keyed to evidence that a serious crime is being or has been committed.

These are welcome assurances. But for the moment, that's all they are. As one conservative Alabama congressman said in a Monday subcommittee hearing, "What you're saying is, 'Trust us.'"

That's the nub of the problem. The ominously named Carnivore is so encompassing, so sophisticated, so tweakable — and its inner workings so closely guarded — that it's almost impossible for anyone besides its operators to know what it's really examining and really ignoring.

This differs markedly from telephone wiretapping. In classic wiretapping, if a tap is to be placed on one phone, agents have traditionally opened a junction box and attached connectors to terminals for that phone and that phone only. In some instances, only incoming and outgoing phone numbers are registered. In others, depending on what a judge thinks is necessary, actual conversations are recorded.

In a sense, comparable service can still be delivered to law enforcement agencies by a customer's Internet service provider. It is reasonably assured that only one client's communications will be looked at.

Carnivore is different. If the service provider allows it to be installed, the Carnivore filter is placed directly in the path of the company's entire Internet data flow. The filter is supposed to "sniff" only what it is set to — for example, incoming and outgoing e-mail addresses for just one account. Or it can probe more deeply. But everything moves through it — from child porn and drug deals to recipes shared with Aunt Nell or strategy discussions between politicians and their policy advisers.

The most comforting observation we've heard so far came from the FBI's Marcus Thomas, a developer of the system. He told The Wall Street Journal that if Carnivore actually were told to read everything that came through, it would bog Internet traffic down to a degree that couldn't go unnoticed. That sounds plausible, a little like trying to force a firehose's output through a soda straw.

Still, the temptation to look at more than what is authorized, whether with good intentions or evil, is powerful. Law enforcement has done it repeatedly in the past, undercutting to some extent the assurances that it won't happen with Carnivore. And the immense power that Carnivore possesses only enhances the pressure to use it.

That's why factions as divergent as extremely liberal and deeply conservative members of Congress, along with the ACLU and many just plain citizens, are nervous about the device. Its technical ability to run afoul of the Fourth Amendment's protections against unreasonable searches is unmistakable.

What this flap points to above all else is that communication technology has far outpaced the nation's wiretap laws, some of which date back to the early 20th century. This is a problem only Congress can address. To its credit and that of the administration, some attempts are in progress.

The administration has asked that federal laws on Internet communications security be upgraded to assure that they match the kind of judicial and administrative restraint that already applies to phone taps. Sen. Patrick Leahy, D-Vt., has written a broad-based Internet privacy bill, and Sen. Orrin Hatch, R-Utah, has introduced another, somewhat narrower measure.

Such attempts, while laudable, will not be reconciled for months, perhaps years. Meanwhile, the FBI has offered to let an independent third party review whether Carnivore's deeds match the agency's words. That would be welcome, but Carnivore ought to be shut down until such a review can be completed and reports issued to Congress.

No modern law enforcement agency should be entirely deprived of surveillance techniques, but putting Carnivore on hold wouldn't do that. It would, on the other hand, provide at least some assurance to innocent parties that their private lives aren't open books. That could hardly be a bad thing.

USA TODAY

DATE: 7-28-00

PAGE: 1

Warrants for online data soar

Demands served on Internet, e-mail providers up 800%, study finds

By Will Rodger, USATODAY.com

The number of search warrants seeking citizens' online data has soared more than 800% during the past few years, a USA TODAY study shows.

The findings, based on an examination of warrants served on the top Net service provider, America Online, surprised federal lawmakers and civil libertarians and prompted calls for legal reforms.

Searches for the online data typically involve cases ranging from harassment and child pornography to violent crime and fraud and are aimed at discovering the identity and tracking the activities of subscribers. Last year, AOL was served with 301 search warrants, up from 33 in 1997. This year, state and local investigators have served 191 warrants through July 17, filings show. AOL had no comment.

All Internet service providers and Web mail providers in the USA "have experienced a significant increase in the number of search warrants and subpoenas," said Andrew Grosso, an attorney who specializes in computer law.

Congressional leaders informed of the findings said they will examine legal standards applied to such Internet investigations. At a minimum, House Majority Leader Dick Armey, R-Texas, said, police need to tell Congress when, why and how they perform electronic searches. The White House already has pledged to move soon to protect electronic data.

Critics and privacy experts fear that electronic surveillance of all types, if not tightly controlled, can violate laws against unreasonable police searches. The FBI's Thomas Gregory Motta says there is little reason for concern.

So far, he says, the law has treated stored records, such as e-mail, as it treats other documents, such as letters and diaries, which can be seized from a home with a simple search warrant. Often, though, authorities ask for more than e-mail.

A random sample of 14 such warrants in the past 18 months showed that 10 asked for all data the service had on targeted subscribers. "They can get a record of what times you dialed in, where you dialed in from, how long you were online, what activities you were engaged in, what Web sites you visited, what chat sessions you were in and what you said there," said Mark Rasch, a former federal prosecutor and vice president for cyber. law at Global Integrity in suburban Washington.

10

Doc 41

July 28, 2000

BARR BILL UPDATES WIRETAP LAWS
MEASURE ENHANCES ELECTRONIC PRIVACY PROTECTION

WASHINGTON, D.C. -- U.S. Representative Bob Barr (GA-7) announced today he was introducing the "Digital Privacy Act of 2000." The legislation updates wiretapping laws to enhance privacy protections and bring them in line with technological developments, such as the Internet, wireless phones, and electronic mail. Specifically, the measure would:

- Extend reporting statues requiring law enforcement to report on its interception of electronic communications, in addition to the telephone wiretap reports already required.
- Block the use of electronic evidence in court if it is obtained illegally.
- Stop unchecked government access to the identities of computer users unless there is reasonable evidence a crime has been committed.
- Stop the government from tracking the location of cell phone users without a court order.

"As the White House recently acknowledged, our wiretapping laws have fallen far behind the technological explosion of the past decade. For example, under current law, e-mails receive less legal protection than both traditional postal mail and telephone conversations," said Barr.

"The Digital Privacy Act corrects some of the most glaring contradictions and loopholes in current law. As systems from NSA's Project Echelon to FBI's Carnivore have proven, technological advances make large scale surveillance easier than ever before. It is vital we safeguard our civil liberties by making certain the law changes to prevent longstanding Fourth Amendment protections from being eroded," Barr continued.

Barr, a Member of the House Judiciary Committee, has served with both the Department of Justice and the Central Intelligence Agency.

--30--

To send a letter to the editor on this topic

To have a regular e-mail update delivered t you.

BACK TO PRESS RELEASES

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

18 Page(s) withheld for the following reason(s): SEALED COURT DOCUMENT FROM USDC CENT DIST. OF CAL. NO. CR99-285(A)-ABC

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #1 (Pages 562 - 579)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

EARTHLINK

FILED
CLERK U.S. DISTRICT COURT
FEB - 4 2000
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA - WESTERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION OF A PEN REGISTER AND TRAP AND TRACE DEVICE.	Criminal No. 99-2713M ORDER: (1) DENYING MOTION TO QUASH ORDER AUTHORIZING PEN REGISTER; AND (2) GRANTING APPLICATION TO EXTEND ORDER AUTHORIZING PEN REGISTER

This case raises the question whether this court has the legal authority under the pen register statute, 18 U.S.C. § 3122, et seq., to issue an order requiring an Internet service provider (ISP) to install a device which captures the time, date, source and destination addressing information of electronic mail (e-mail) messages sent to and from an e-mail address maintained by a customer at the ISP. After consideration, the court finds that it has the legal authority under the pen register statute to issue such an order.

The discussion of this issue arises in the context of an ongoing criminal investigation. The court does not want to compromise the integrity of that criminal investigation. Accordingly, the description of the facts out of which the current dispute arises deliberately omits factual information which could alert the subject

Doc. #2

or subjects of the investigation to the existence of and the techniques used in the investigation.

On December 2, 1999, the government, through an Assistant United States Attorney, presented to the court an ex parte application for the issuance of an order in the nature of a pen register. The application contained information that a federal criminal investigatory agency was seeking to locate a federal fugitive, that agents of the federal agency believed that the fugitive was maintaining contact with a specific named close friend or relative ("the subject") by means of e-mail transmissions sent to the subject, and that the subject maintained an Internet service account with a designated Internet service provider ("ISP") under the subject's name. This court issued an order providing that the government agency "may install a pen register and trap and trace device to register time, date, and source and destination addressing information of the electronic mail messages sent to and from the subject Internet account, including information regarding the true source of the messages without geographic limitation."

The government agency served the order on the ISP. The ISP and the government had some initial discussion regarding the order. Eventually, the ISP attempted to comply with the order by providing the agency with the "headers" (minus the subject or regarding line) of numerous incoming messages to the subject's e-mail account and the "headers" of a few outgoing messages (with the subject or regarding information deleted) from the subject account. The government is not satisfied with this response, contending that the terms of the order entitle it to install its own device on the premises of the ISP connected to ISP's equipment.

5/24/02 Release - Page 581

02/09/00 11:05 FAX 213 894 6268 US ATTORNEY OFFICE 003

As a result of this dispute, the ISP has now moved to quash or modify the order. The government has opposed the motion to quash and separately submitted an ex parte application requesting an extension of the court's previous order.

At an initial scheduling conference, the parties represented that the court's original Order, issued December 2, 1999, would expire February 4, 2000. This court scheduled a hearing on the ISP's motion to quash or modify the order on February 4, 2000. It now appears to the court that the order has already expired. The statute provides that the court may issue an order authorizing the installation of a pen register "for a period not to exceed 60 days." 18 U.S.C. § 3123(c)(1). The Order was issued on December 2, 1999. Pursuant to the terms of the statute, the Order expired 60 days thereafter on January 31, 2000.

There is no presently effective order in place which this court may quash. The court therefore denies the ISP's motion to quash as moot.

Although that ruling resolves the pending motion of the ISP to quash, it does not resolve the underlying issue whether the court has the authority to issue an order. That issue is now presented to the court because the court must decide the government's application to extend the order.

The statute provides that:

> "the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified

02/09/00 17:08 FAX 212 894 4260 US ATTORNEY OFFICE 004

to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."

18 U.S.C. § 3123(a).

The government has certified to the court that the information likely to be obtained by the pen register or trap and trace device is relevant to an ongoing criminal investigation. This court accordingly has authority to issue a proper pen register or trap and trace order. The question presented here is whether the device which the government seeks to install is a device described and authorized in the statute.

The statute defines a "pen register" as:

"a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached . . . ."

18 U.S.C. § 3127(3).

The statute describes a "trap and trace device" as:

"a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."

18 U.S.C. § 3127(4).

It is apparent that a pen register, as defined in the statute, is intended to be a device which captures the telephone numbers dialed by a target phone. A trap and trace device is intended to capture the telephone numbers of telephones which make calls to a target phone. It is also fairly clear that the drafters of the pen

02/08/00 17:08 FAX 213 894 8268 US ATTORNEY OFFICE 005

register statute did not contemplate that the statute would be used to authorize the issuance of court orders to capture the e-mail addresses of persons sending e-mail to and receiving e-mail from a targeted e-mail address.

The statutory definition of a pen register describes a device attached to a telephone line. 28 U.S.C. § 3127(3). The statutory definition of a "trap and trace device" does not limit the description to a device attached to a telephone line. 28 U.S.C. § 3127(4). "Nonetheless, it appears from the construction of related sections of the statutes governing trap and trace devices that they include only devices that are attached to a telephone line." In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F.Supp. 197, 200 (C.D. Cal. 1995) (hereafter "In re Cellular Digital Analyzer"). An order for use of both pen register and trap and trace devices must include "the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached . . . ." 18 U.S.C. § 3123(b)(1)(C).

It is clear that the government here does not intend to attach either a conventional pen register or a trap and trace device to the subject's telephone line. The government's opposition to the ISP's motion to quash contains a description by a technician declarant of how the government intends to implement the requested order. The government would install a computer program called "Carnivore" on the ISP's network, probably on a "router" used by the ISP. A "router" is described as a transmission device that processes packetized network information. Both the router and the ISP's network are connected to the telephone lines and transmit packetized network information over

02/09/00 17:08 FAX 213 894 6268 US ATTORNEY OFFICE 006

telephone lines. The Carnivore software program would look for the target's log-in name (presumably for outgoing e-mail) or the target's electronic mail name (presumably for incoming e-mail). The program would then capture the "header" information associated with the e-mail message, including the time, date, and addressing information, including Internet identity, for messages sent to or from the target account. The program would not capture the subject or regarding line of the e-mail message or the content of the message. The captured material would be stored on a government computer which presumably would be attached to the ISP's router.

A conventional pen register is attached to telephone lines and captures the telephone number dialed by the target telephone. A trap and trace device is attached to telephone lines and captures the telephone numbers calling the subject telephone. Here, the government's requested device is a computer and software program attached to the ISP's equipment which is, in turn, connected to telephone lines and which captures the Internet e-mail addresses of persons sending to or receiving e-mail from the target. There appears to be no significant difference between capturing telephone numbers with a pen register or trap and trace device and capturing e-mail addresses with the government's proposed computer and software program.

This court acknowledges that the pen register statute, 18 U.S.C. § 3122, et seq. is contained in Title III of the Federal Electronic Communications Privacy Act of 1986, that one of the evident purposes of that statute is to regulate government intrusion into private communications, and that the statute should be strictly construed. In re Cellular Digital Analyzer, 885 F.Supp. at 200. This

court finds that the intrusion into otherwise private activity which would be allowed by the issuance of the government's requested order is no greater than the intrusion created by the issuance of a conventional pen register order. Although apparently not contemplated by the drafters of the original statute, the use of a pen register order in the present situation is compatible with the terms of the statute. Accordingly, the court will grant the government's application for the continued use of a pen register and issue an appropriate order.

For the reasons stated above, the ISP's motion to quash the original order authorizing the installation of a pen register is denied as moot. The government's application for the continued use of a pen register is granted.

IT IS SO ORDERED.

DATED: February 4, 2000

JAMES M. McMAHON
United States Magistrate Judge

02/09/00 11:07 FAX 212 884 8289 US ATTORNEY OFFICE 009

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

4 Page(s) withheld for the following reason(s): SEALED COURT DOCUMENT FROM USDC CENT. DISTRICT OF CALIFORNIA NO. 00-0249M

X The following number is to be used for reference regarding these pages: DOCUMENT #3 (Pages 587-590)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

UNITED STATES MARSHALS SERVICE
Investigative Services Division
Electronic Surveillance Unit

Office: (703) 285-3200, Facsimile: (703) 285-3215

b6-1
b6-3
b7c-1
b7c-3

TO: [redacted]

FROM: [redacted]

DATE: 02/02

NUMBER OF PAGES: 18 EXCLUDING COVER SHEET

COMMENTS:

WARNING: MANY FACSIMILE MACHINES PRODUCE COPIES ON THERMAL PAPER. THE IMAGE PRODUCED IS HIGHLY UNSTABLE AND WILL DETERIORATE SIGNIFICANTLY IN A FEW YEARS. IT SHOULD BE COPIED ON A PLAIN PAPER COPIER PRIOR TO FILING AS A RECORD.

Doc. #4

UNITED STATES MARSHALS SERVICE

Office of the Assistant Director for Investigative Services
600 Army Navy Drive
Suite 1200 - Crystal Square 4
Arlington, VA 22202
Phone: (202) 307-9110
FAX: (202) 307-9299 or (202) 307-9337

To: Marcus Thomas	Fax #:
From: [redacted]	
Date: 02/07	
Number of Pages: (excluding cover sheet) 5	

b6-3
b7C-3

MESSAGE:

Call me with any questions

[redacted]

Thanks

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

7 Pages were not considered for release as they are duplicative of DOCUMENT #2 OF THIS FILE

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #4, PGS. 3-9 (Pages 593 – 599)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

DECLARATION

I Edward Hill hereby declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been an Agent for 10 years. I specialize in technical equipment, including electronic surveillance equipment. I am familiar with the Internet and with surveillance devices used for the Internet.

2. If authorized by this court, I or other technicians intend to install a program called Carnivore to obtain the information sought in this order. The program will be installed on EarthLink's network, most likely on a "router" used by EarthLink. A "router" is a transmission device that processes packetized network information. Both the router and EarthLink's network are connected to the telephone lines and transmit packetized network information over the telephone lines. The Carnivore software program watches the incoming telephone traffic to EarthLink and looks for the targeted subscriber's log-in name or electronic mail account name. If it finds the target's log-in name, the program follows the target while the target is on line. The program then captures only the header information for electronic mail messages sent or received by the target while the target is on line. If the program finds the target's electronic mail account name, it will capture the header information associated with that electronic mail message. Specifically, the program will capture the time, date, and the addressing information (i.e., Internet identity) for electronic mail messages sent to or from the account. The program will not

capture the subject or regarding line on the electronic mail message, nor does it capture the content of the message or any information concerning the target's other on line activity.

3. Although the program is capable of capturing more than the information authorized under the order, I or the installing technicians will configure the program in a manner that will prevent the program from capturing any information that is not authorized under the order. In addition, the computer used to run the program has limited memory capacity and limited ability to process information. Because of these limitations the computer used to run the program would be overloaded within a few minutes if it attempted to collect all of the information on EarthLink's 8 to 10 million e-mail messages. Moreover, the program will be installed on a particular entry point into EarthLink's network, and as such would not have access to all of EarthLink's customers.

4. The program should not create a security risk for EarthLink. Although the Carnivore program is remotely accessible, it has several security provisions that prevent an intruder from obtaining unauthorized access to EarthLink's system. Even if an intruder did obtain such access, the program lacks a TCP/IP protocol stack, which means that the intruder would be unable to communicate with EarthLink's system from the government's computer. I and other agents with whom I work have installed this program at many other service providers (including AT&T) and have not had security problems or objections from the providers.

6C-1
67C-1

From: [redacted]
To: BOWMAN, SPIKE (MARION) [redacted]
Date: 4/5/00 5:29PM
Subject: [redacted]

I just received a call from [redacted] at OIPR. To state that she is unhappy with ITOS and the UBL Unit would be an *understatement* of incredible proportions. I will try to relate what [redacted] thinks has happened with the above named FISA.

[redacted] secured an ELSUR FISA very quickly on [redacted] at the request of [redacted] states that she was assured that the FBI had special software which could do what the FBI said it could do. In fact [redacted] states that the technical people in Quantico approved the FISA language.

The FBI technical people went to install the FBI software a[redacted]o accomplish the electronic surveillance on March 16.

The software was turned on and did not work correctly. The FBI software not only picked up the E-Mails under the electronic surveillance of the FBI's target, [redacted] but also picked up E-Mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [redacted] is under the impression that no one from the FBI [redacted] was present to supervise the FBI technical person at the time. Now the FBI technical people want to run a new software experiment at the carrier to see if it works.

[redacted] states that OIPR was never told that the FBI software was experimental. OIPR was informed that it would work. The FBI technical people are still trying to make it work in [redacted], and want to resume the electronic surveillance. The FBI people in [redacted] also want a physical search warrant to pick up the E-Mails from the carrier, which the FBI picked up on the target, but destroyed.

[redacted] informed me that the FBI does not have the authority to resume electronic surveillance until she receives a written explanation of what has happened and she files something with the court. Obviously, she has no intention of securing a search warrant either until this is straightened out.

When you add this story to the FISA mistakes covered in the E.C. I have prepared to go to the field, and which is in NSLU for signature before it goes to [redacted] for his signature, you have a pattern of occurrences which indicate to OIPR an inability on the part of the FBI to manage its FISAs.

[redacted] and [redacted] please see me ASAP.

Thanks
[redacted]

CC: [redacted]

6C-2
6C-1
6C-3
67C-1
67C-3

DOC. #5

From: [redacted]
To:
Date: Tue, Apr 11, 2000 9:00 AM
Subject: DITU Legal Issues

[redacted]

The attached sets out a few issues we would like to discuss with you so that we can work toward providing a reasonalbe and practical guideline to personnel in our Unit and the Field.

My number is 703[redacted] I will be on leave from Thursday through next Tuesday.

CC: [redacted] MARCUS C THOMAS

b6-1
b7C-1

Doc. #6

[redacted] 6C-1 67C-1

The following sets out some of the legal issues facing DITU as well as some thoughts on ways to proceed. We need your legal guidance in this matter to formulate a reasonable and prudent course of action, as well as a practical working guide for the personnel of DITU and the Field Office personnel involved in Data Intercepts. I am sure there are other issues and ideas, but this may be a good start. Call me to discuss this in more detail. I am willing to travel to your office at FBIHQ or to meet with you here at QT. If you need any clarification of technical concepts etc. you may call SSA [redacted] at 703-[redacted] or SSA [redacted] at 703 [redacted] 6C-1 67C-1

To initiate an intercept on a network or at an ISP, the DITU installs a collection device with appropriate filters set to capture data within the scope of the Court Order or the effective consent of a consenting party. This filtering process, a component of Etherpeek and Carnivore, filters based on TCP/IP standards. On occasion we encounter non-standard implementation of transmission control and Internet protocols within a network or at an ISP. Encountering non-standard implementation has led to inadvertently capturing and processing data outside the Order or Consent.

Issue I

In instances where we encounter non-standard implementation of a protocol which leads to the improper capture of data, two main concerns arise. The first, and of most immediate concern, is the formulation of a guideline to be followed in resolving the matter. This guideline should extend from the DITU personnel who installed and likely discovered the error, through DITU Management representatives, Field Division Case Agents, CDCs, notifications to AUSAs, Motions to Seal, etc.

Issue II

The second issue, critical in efforts to intercept the data under the Court's Order or under consent from a test account, is how FBI technical personnel, such as, Engineers, Computer Programmers and others, may lawful examine the collected data for the sole purpose of determining why the filters failed and what software changes need to be made to bring the collection in line with the scope of the existing Order. We need to look at the data to figure out what is wrong and how to fix it!!!

Issue III

A third issue which we would like you to consider is that we frequently set up user accounts on networks and install data intercept devices to perform a "test tap" under our own consent. This is generally done as a means of verifying that the location on the network and the filter set would be appropriate for an anticipated or existing intercept Order. In the event that we are doing a "test tap" under consent, looking for our own mail, etc, and inadvertently capture something outside our consent, such as another persons mail, what are our options? Is it a violation of TIII if the interception is not intentional and we do not disclose or endeavor to disclose the information to anyone? May we destroy the information and simply not disclose it to anyone?

Issue IV

Random Access Memory RAM

In relation to the "testing" of network placement and filters, it is generally a technical requirement to install the device with appropriate filters set and initiate the capture process. It may be hours or days before a determination can be made as to the functional operation of the collection. During these first few hours or days, the technical representatives of the FBI, Electrical Engineers, Electronics Engineers, Technically Trained Special Agents and others may frequently examine collected data to determine the efficacy of the installation. In relation to the time period from installation to the verification of proper function, the following question is posed for your consideration. Is there a significant legal difference between Random Access Memory (RAM), that which is not retained when power is removed, and of a hard-drive or floppy disk which retains the data. The thought process here in the DITU being that: during the period of time from the installation to the verification of proper function, the data could be directed to remain in RAM and not be forwarded to a permanent media. Technical representatives could then examine the collected data for proper filtering and

assure that the collection is operating within the scope of the Order.

If the collection appears technically correct, it could then be re-directed from RAM to permanent media and the intercept initiated. If not, the data could be examined in RAM by Computer Programmers/Engineers to determine a filtering change or software patch necessary to effect the Court Ordered intercept. The data in RAM would not be retained by the computer on power-off.

By directing collected data to remain only in RAM, we may gain both the ability to troubleshoot installations and to assure that the data is not written to "storage media" nor recoverable from any media.

66-1
67E-1

From: [redacted]
To: [redacted] THOMAS, MARCUS C
Date: Wed, Apr 12, 2000 5:53 PM
Subject: ISP INTERCEPTS E-MAIL

See the attached. After you all get a chance to review my initial thoughts regarding your questions/issues, let's then plan to sit down and talk.

TX

[redacted]

Doc. #7

4/12/2000

TO: Marcus Thomas
[redacted]

FROM: [redacted]

RE: Internet/E-Mail Intercepts

This is in response to [redacted] E-mail of 4/11 regarding the captioned matter.

b6-1
b7C-1

The following are some preliminary reactions and thoughts. They are not necessarily final legal answers or guidance. They are offered to stimulate further consideration on all of our parts. As was suggested in the E-mail, we all need to sit down in the very near future and take a little time to talk about our intercept approaches, as well as what we must do when they unintentionally go astray.

Background:

We need to start with a few high-level and familiar thoughts, because they form a background and context for the subsequent discussion. As we are all aware and appreciate, electronic surveillance is a very sensitive investigative (and intelligence/counterintelligence) technique.[1] As such, for over 30 years, it has been carefully regulated by and through statutory regimes at both the Federal and State levels -- which regimes, in many instances, contain provisions that are very specific, and which contain dictates that are quite detailed in their procedural/administrative aspects. On its face, the language of these regimes, as written by the Congress, is essentially black and white, and generally is unforgiving: one complies with the statutes or, alternatively, violates them. In enacting these regimes, Congress sought to balance and advance privacy and effective law enforcement. Moreover, given the sensitivity of this technique, electronic surveillance has been the subject of on-going scrutiny by Congressional oversight committees, the press, privacy groups, and the public. In short, there are few, if any, investigative techniques that are (and have been) subjected to such heightened scrutiny. And there are few, if any, investigative techniques that garner (and have garnered in the past) such vehement criticism when errant surveillances or missteps (be they intentional or unintentional) occur.

While, as noted above, the electronic surveillance laws are often specific and detailed in their provisions, generally they do not address the precise aspects of how, technical speaking, the "intercept" is to occur. Congress eschewed doing so because it would be a bad idea to try to delineate all the various potential interception methodologies/approaches. To do so would infringe upon Executive Branch prerogatives in "executing" the laws. And, it would get into sensitive intercept sources and methods, etc. Nevertheless, both the Congress and the courts have

---

[1] While we in our particular area of law enforcement are so close to this matter that we literally live and breathe electronic surveillance, to others (especially those outside of law enforcement), *any electronic surveillance is a big thing!*

an extremely keen interest in making sure that several things are being attended to by the Executive Branch in conducting electronic surveillance searches and seizures: (1) that illegal, unconstitutional searches are not occurring (i.e., that no searches of persons' communications are occurring without probable cause/warrant/emergency); and (2) that the spirit/intent/letter of the electronic surveillance laws (as implementers of constitutional law -- at least to a degree) are being carried out carefully and judiciously. One aspect of this involves the requirement that such surveillances only be approved with high-level departmental approval and with on-going Departmental legal/administrative oversight.

Interceptions of the "Older" Communications Technology

It is probably fair to say that, historically, Congress has been of the opinion (and correctly so) that, for law enforcement, effecting a lawful interception was not a particularly problematic endeavor. Typical wire line service lent itself to reasonably easy segregation of a target's communications to the target line,[2] and thus to concomitantly effecting lawful (and effective technically-targeted) interceptions. With other identifiers (ESNs, MINs, Cap Codes, etc.) being available, accurately targeted interceptions of cellular phones and pagers could likewise be effected by law enforcement. Importantly, Congress understood that, in order to effect accurate interceptions, law enforcement would seek and obtain assistance from electronic communication service providers (ECSPs) and/or others to properly conduct the intercept ("...upon request [of an ECSP, it shall] furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception ... with a minimum of interference with the services [the ECSP is according to] the person whose communications are to be intercepted"). 2518 U.S.C. 2518(4). Until 1994 (*see* below), there is no clear indication, in the statutes or otherwise, that Congress ever understood *interception accuracy* to be an issue for law enforcement.

Where potential "over-acquisitions" could arise, Congress, privacy groups, and others have homed in and taken an interest. For example, with regard to pen register/DNRs, Congress and others have been concerned about certain (but not all) post cut-through dialing -- i.e., certain dialing that arguably constitutes a substantive communication -- even though related to the target individual (as opposed to communications of others). In this regard, Congress, as part of the CALEA legislation, specified in 18 U.S.C. 3121(c) that law enforcement "shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing." Similarly, under CALEA's assistance capability requirements, Congress specified, as a statutory requirement as part of the interception capability, that telecommunications carriers meet their obligation "in a manner that

---

[2] One possible exception being "party-line" service, which by now is pretty rare. Its unclear exactly what Congress would think about such party-line-related intercepts. Presumably, minimization could be employed to parse the target subscriber's calls. But, at the end of day, under the statutory regime/language, the telephonic communications being targeted for interception would, in fact, be occurring over the properly-targeted telephone line/facility. Here, law enforcement would, at least, be on the correct line/facility that had been authorized for interception by the court.

protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted...." 47 U.S.C. 1002(a)(4)(A).

Internet and E-mail Service Providers

Both Internet Service Providers (ISPs) and E-mail service providers are comprehended within the term "providers of 'electronic communication service'" under the ECPA and Title III/FISA. *See, e.g.*, 18 U.S.C. 2510(15). Moreover, certain facets of E-mail/ISP service, at least with regard to the acts of transmitting and routing wire/electronic communications, can also constitute activity of a "telecommunications carrier," thereby subjecting the communications/carrier to the provisions of CALEA. *See* 47 U.S.C. 1001(8). Accordingly, certainly under the ECPA/Title III/FISA (and perhaps under CALEA), such electronic communication service providers are mandated to afford all the necessary assistance to properly effectuate an interception of electronic communications. Consequently, whenever there is an electronic surveillance order, and whenever there are any questions about "standard/non-standard transmission control(s)," "protocols," or any other technical information matter of consequence in properly and accurately effecting electronic surveillance, these service providers are duty-bound to work with us in properly and lawfully effecting the surveillance order.

Internet/E-mail Interceptions

In the referenced DITU E-mail, it is explained that certain Etherpeek and Carnivore "filters" are utilized to (hopefully) capture data (and only that data) authorized for interception in an electronic surveillance order or pursuant to consent. The E-mail mentions that, on occasion, when non-standard implementations have been encountered, data outside the court order or consent have been captured and processed inadvertently. DITU then presents several issues for examination. In the first two, DITU (1) seeks guidance as to formulating guidelines for reacting to such inadvertent interceptions and (2) whether additional examination of such non-authorized data is permitted to remedy the errant collection/filtering efforts.

As noted in the background comments, the electronic surveillance statutes speak at a rather high level, and are essentially black and white in nature -- with one either complying with the law or facially violating it. The Title III statutes, generally speaking, are not "specific intent" statutes. That is, one does not need to have *special* or *particular bad intention* or *motive* to facially violate the law. Further, since the protection of personal communications privacy is a key facet of the statutory purpose and regime, any unauthorized interception of another's communications is a matter of concern (at a minimum). Indeed, some might argue that the government's unauthorized interception of such communications is even more problematic.

Historically, as a matter of Departmental practice/policy, unauthorized interceptions (be they of the subject of the interception or others) have been taken seriously by DOJ (and by the FBI for that matter). When detected, DOJ has advised AUSAs to (1) file a pleading with the court explaining the unintentional/intentional act and to (2) seal the unauthorized intercepted communications with the court, in order to prevent further harm such as subsequent use or disclosure (*see* 18 U.S.C. 2511(1)(c)(d), 2515). Such unauthorized interceptions not only can

5/24/02 Release - Page 6 1

violate a citizen's privacy but also can seriously "contaminate" ongoing investigations. In addition, DOJ could also counsel the AUSA to recommend/not recommend to the court whether or not the person(s) who communications were improperly intercepted should be notified.

Interestingly, under Section 2511(2)(a)(ii), while Title III specifies that "no [criminal] cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification [under Title III]," there is no similar explicit protection for law enforcement personnel under this provision. Now, practically speaking, there is virtually no chance that law enforcement officers acting in good faith, pursuant to a court order, are going to be criminally prosecuted (or even investigated)! As to civil liability, under 18 U.S.C. 2520(d), Title III states that "a good faith reliance on ... a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization... is a complete defense against any civil or criminal action brought under [Title III] or any other law." So, here too, law enforcement personnel should be immune, practically speaking, from any liability. (Further, even if (in a semi-egregious case) liability were to be found, it would almost certainly fall to the agency -- not the agent/support personnel.) However, the FBI itself routinely does conduct OPR-type inquiries, from an administrative perspective, in order to determine the nature/cause, etc. of any investigative missteps or errors which facially violate a law, with an eye toward preventing future reoccurrences, etc.

In a similar fashion, missteps under FISA lead to mandatory reporting to the President's Foreign Intelligence Advisory Board (PFIAB), and such errancies must be reported/explained/justified to Congress.

Issue #1:

In short, then, as to the first issue, upon detecting an inadvertent, unauthorized (unlawful) interception:

A) the technical effort that is causing the mistake should be stopped immediately (and not re-instituted until advised to do so by the supervising attorneys);
B) the error should be reported immediately to the FBI substantive case personnel in the field/headquarters (as appropriate), to the field office TA and CDC, and to the respective AUSA/OIPR supervisory attorney (who, in turn, will presumably advise the court);
C) the reporting as to the errant interception should be careful and clear so that those to whom it is reported will fully understand what happened; the reporting should not include any substantive aspect of the *content* of the communication that may have been gleaned; and
D) the unauthorized intercepted material should be segregated immediately as a prelude to formal sealing with the court.

Issue #2:

As to "examining" the unauthorized intercepted data (albeit for the sole purpose of determining why the filters failed and what changes need to be made), this is a very delicate and potentially

problematic area. It would appear that continuing to look at (examine and "use") the substantive content/plain text of the material that was not authorized for interception would most aggravate Title III's concerns/dictates (*see* Sections 2511 and 2515), and most likely would *heighten* the legal problem in the minds of the Department, FBI-OPR, the court, Congress, privacy groups, the public, etc. If, on the other hand, there is some way of looking at the signaling, programing, protocols, etc. *in a raw/unintelligible state (I can amplify later)*, this might be okay if (1) it is for the sole purpose of determining why the filters failed and what changes need to be made, and if (2) it is approved by the AUSA/OIPR (and/or the court if the AUSA/OIPR believe warranted -- such court permission in this area would presumably be preferable from the perspective of legal protection for our technical people). Another thought I would strongly encourage is to engage the ISP. That is, if there is a technical (filter) failure problem regarding the interception, it would appear to be much much more preferable for the ISP to try to fix it (even with us coaching and/ or guiding technically from afar). The reason for fully utilizing the ISP is the existing mandate for their assistance, etc. under the law, and because of the "cover" it affords us legally, politically, and perceptionally.

Issue #3:

DITU poses a similar issue as to one its own "test" accounts where an inadvertent, unauthorized interception occurs. Again, we have to be very careful here, even where "testing" is our activity, because the potential harm/violation of privacy is arguably the same. Somehow, when we test, we have to go out of our way to avoid tripping over innocent third party communications. I am not sure how we can proceed to test without inadvertently intercepting the communications of others, but we really need to try. Perhaps, we can explain our testing requirement to the ISP and get them to test our filters, etc. for us, since it is *their* network, and since *they* administrate it, etc. anyway. I would really encourage using the ISPs for many reasons, not the least of which is to make them aware of us popping around in their network to conduct testing, etc.

Issue #4:

DITU asks whether interception collections effected in Random Access Memory (RAM) (rather than permanent media) make any significant legal difference. In short, I would say probably not as a purely legal matter, inasmuch as an unauthorized interception is, after all, an unauthorized interception. Now, having said that, it may make some feel better that the potential for ongoing "use" and "disclosure"(through some permanent storage media) may be somewhat reduced -- but I don't think this is the path to take. As alluded to above, I would opt for more controlled testing and utilizing service providers as much as possible to create some insulation between us and the subscriber public where inadvertent interceptions might arise in the course of our trying out our filters, etc.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of DOC #1, OGC/TECHNOLOGY LAW UNIT FILE (PAGES 155-157)

_____ Page(s) withheld for the following reason(s): _____

_____

_____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #8 (Pages 614-616)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

6C-1
67C-1

FBI Using Internet Wiretap System (washingtonpost.com)
By John Schwartz
Washington Post Staff Writer
Tuesday, July 11, 2000; Page A1

The FBI has deployed an automated system to wiretap the Internet, giving authorities a new tool to police cyberspace but drawing concerns among civil libertarians and privacy advocates about how it might be used.

The new computer system, dubbed "Carnivore" inside the FBI because it rapidly finds the "meat" in vast amounts of data, was developed at FBI computer labs in Quantico, Va., and has been used in fewer than 50 cases so far.

But that number is sure to rise, said Marcus Thomas, chief of the FBI's cyber-technology section at Quantico. "In criminal situations there's not yet been a large call for it," he said, but the bureau already has seen "growth in the rate of requests."

Civil liberties groups said the new system raises troubling issues about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, the new technology also could scan private information about legal activities.

"It goes to the heart of how the Fourth Amendment and the federal wiretap statute are going to be applied in the Internet age," said Marc Rotenberg, head of the Washington-based Electronic Privacy Information Center.

The new system, which operates on off-the-shelf personal computers, takes advantage of one of the fundamental principles of the Internet: that virtually all such communications are broken up into "packets," or uniform chunks of data. Computers on the Internet break up e-mail messages, World Wide Web site traffic and other information into pieces and route the packets across the global network, where they are reassembled on the other end.

FBI programmers devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

The ability to distinguish between packets allows law enforcement officials to tailor their searches so that, for example, they can examine e-mail but leave alone a suspect's online shopping activities. The system could be tuned to do as little as monitoring how many e-mail messages the suspect sends and to whom they are addressed û the equivalent of a telephone "pen register," which takes down telephone numbers being called without grabbing the content of those calls.

"That's the good news," said James Dempsey, an analyst with the Center for Democracy and Technology, a Washington high-tech policy group. "It is a more discriminating device" than a full wiretap, he said.

But Dempsey expressed worries about the new system, which would be

DOC # 9

b6-1
b7C-1

from pen-register data to full wiretaps with court authorization. "It's not an increase in our authority; it doesn't present a change of volume in what we do," he said.

© 2000 The Washington Post Company

6C-1
67C-1

FBI e-mail Snooping Device Attacked

July 11, 2000

Filed at 7:26 p.m. EDT
By The Associated Press
WASHINGTON (AP) -- Civil liberties and privacy groups railed Tuesday against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.
The system, called ``Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.
When Carnivore is placed at an Internet Service Provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.
In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.
Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.
``Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target,'' read the letter. ``This 'trust us, we are the government' approach is the antithesis of the procedures required under our wiretapping laws.''
Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping data-tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, is already intrusive.
``Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target,'' Steinhardt said in an interview. ``When conducting these kinds of investigations, the information should be restricted to only addressing information.''
A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the Constitution subcommittee, said that the congressman had no immediate comment on the letter.
In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law firm in Washington, said that he represented

Doc #10

b6-1
b7C-1

an Internet provider that refused to install the Carnivore system. The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared suits from customers unhappy with the government looking in to all the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents,'' Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost their court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said that the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said that the main problem with Carnivore is it's mystery.

``The FBI is placing a black box inside the computer network of an ISP,'' Dempsey said. ``Not even the ISP knows exactly what that gizmo is doing.''

But Dempsey said that Internet providers contributed to the problem, by saying that current technology does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

``The service providers said they didn't know how to comply with court orders,'' Dempsey said. ``By taking that position, they have hurt themselves, putting themselves into a box.''

Marcus Thomas, who heads the FBI's Cyber Technology Section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

``This is just a specialized sniffer,'' Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, and it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely -- show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

``The FBI should make this gizmo an open-source product,'' he said. ``Then the secret is gone.''

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

b6-1
b7c-1

American Civil Liberties Union: http://www.aclu.org
Center for Democracy and Technology: http://www.cdt.org
Pretty Good Privacy (PGP): www.pgp.com

Copyright 2000 The New York Times Company

Jul 11 2000 11:55 P.01

WALL STREET ARTICLE

[redacted] 64-1

FACSIMILE COVER SHEET
FAX NUMBER [redacted]

Number of Pages 6 *(Including Cover)*

Date: 7/11/00

To: Marcia Thomas

Phone:

FAX: 703-632-6081

From: [redacted] b6-2

Phone: 703- [redacted] b7C-2

Comments:

DOC # 11

Set up your daily schedule on one screen - Free download
New MSNBC.com Personal Update for Microsoft Outlook® 2000
ONLINE RESOURCES FOR SMALL BUSINESSES
MSNBC.COM SMALL BUSINESS

FBI's system to covertly search e-mail raises privacy, legal issues

By Neil King Jr. and Ted Bridis
THE WALL STREET JOURNAL

WASHINGTON, July 11 — The U.S. Federal Bureau of Investigation is using a superfast system called Carnivore to covertly search e-mails for messages from criminal suspects.

COMPLETE STORY

ADVERTISING ON MSNBC

Book Travel Smarter
TRIPS AIR CAR HOTEL VACATIONS MORE...
Join 4.5 million other smart travelers.

NEW MSNBC.com Personal Update for Microsoft Outlook® 2000
Free Download

Learn more about The Wall Street Journal Interactive Edition.

ESSENTIALLY A PERSONAL COMPUTER stuffed with specialized software, Carnivore represents a new twist in the federal government's fight to sustain its snooping powers in the Internet age. But in employing the system, which can scan millions of e-mails a second, the FBI has upset privacy advocates and some in the computer industry. Experts say the system opens a thicket of unresolved legal issues and privacy concerns.

The FBI developed the Internet wiretapping system at a special agency lab at Quantico, Va., and dubbed it Carnivore for its ability to get to "the meat" of what would otherwise be an enormous quantity of data. FBI

technicians unveiled the system to a roomful of astonished industry specialists here two weeks ago in order to steer efforts to develop standardized ways of complying with federal wiretaps. Federal investigators say they have used Carnivore in fewer than 100 criminal cases since its launch early last year.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks. That would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing.

The system also troubles some Internet service providers, who are loath to see outside software plugged into their systems. In many cases, the FBI keeps the secret Carnivore computer system in a locked cage on the provider's premises, with agents making daily visits to retrieve the data captured from the provider's network. But legal challenges to the use of Carnivore are few, and judges' rulings remain sealed because of the secretive nature of the investigations.

Internet wiretaps are conducted only under state or federal judicial order, and occur relatively infrequently. The huge majority of wiretaps continue to be the traditional telephone variety, though U.S. officials say the use of Internet eavesdropping is growing as everyone from drug dealers to potential terrorists begins to conduct business over the Web.

News from the WSJ

Wall Street Journal stories on MSNBC

• Click here to bookmark

The FBI defends Carnivore as more precise than Internet wiretap methods used in the past. The bureau says the system allows investigators to tailor an intercept operation so they can pluck only the digital traffic of one person from among the stream of millions of other messages. An earlier version, aptly code-named Omnivore, could suck in as much as to six gigabytes of data every hour, but in a less discriminating fashion.

Still, critics contend that Carnivore is open to abuse.

Mark Rasch, a former federal computer-crimes prosecutor, said the nature of the surveillance by Carnivore raises important privacy questions, since it analyzes part of every snippet of data traffic that flows past, if only to determine whether to record it for police.

"It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring," Mr. Rasch said. "You develop a tremendous amount of information."

"It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring," Mr. Rasch said. "You develop a tremendous amount of information."

Others say the technology dramatizes how far the nation's laws are lagging behind the technological revolution. "This is a clever way to use old telephone-era statutes to meet new challenges, but clearly there is too much latitude in the current law," said Stewart Baker, a lawyer specializing in telecommunications and Internet regulatory matters.

Robert Corn-Revere, of the Hogan & Hartson law firm here, represented an unidentified Internet service provider in one of the few legal fights against Carnivore. He said his client worried that the FBI would have access to all the e-mail traffic on its system, raising dire privacy and security concerns. A federal magistrate ruled against the company early this year, leaving it no option but to allow the FBI access to its system.

"This is an area in desperate need of clarification from Congress," said Mr. Corn-Revere.

"Once the software is applied to the ISP, there's no check on the system," said Rep. Bob Barr (R., Ga.), who sits on a House judiciary subcommittee for constitutional affairs. "If there's one word I would use to describe this, it would be 'frightening.'"

Marcus Thomas, chief of the FBI's Cyber Technology Section at Quantico, said Carnivore represents the bureau's effort to keep abreast of rapid changes in Internet communications while still meeting the rigid demands of federal wiretapping statutes. "This is just a very specialized sniffer," he said.

He also noted that criminal and civil penalties prohibit the bureau from placing unauthorized wiretaps, and any information gleaned in those types of criminal cases would be thrown out of court. Typical Internet wiretaps last around 45 days, after which the FBI removes the equipment. Mr. Thomas said the bureau usually has as many as 20 Carnivore systems on hand, "just in case."

Advertisement
Shop @ MSNBC

Click here for special deals
Quick Gifts
GO

FBI experts acknowledge that Carnivore's monitoring can be stymied with computer data such as e-mail that is scrambled using powerful encryption technology. Those messages still can be captured, but law officers trying to read the contents are "at the mercy of how well it was encrypted," Mr. Thomas said.

Most of the criminal cases where the FBI used Carnivore in the past 18 months focused on what the bureau calls "infrastructure protection," or the hunt for hackers, though it also was used in counterterrorism and some drug-trafficking cases.

Copyright © 2000 Dow Jones & Company, Inc. All Rights Reserved.

TOP WSJ STORIES ON MSNBC

STORY AOL's assault on Latin America hits a snag with local providers
STORY Deutsche Telekom makes overtures to acquire VoiceStream Wireless
STORY Dell halts the sale of WebPC line
STORY Microsoft aims to sell developers on its new computing platform
STORY Fast-food franchise bank loans fall out of favor with lenders
STORY Ready to list? Selecting where has become tricky in Europe

TOP BUSINESS NEWS

STORY Deutsche Telekom makes overtures to acquire VoiceStream Wireless
STORY Tipping the scales both ways in Microsoft case
STORY Yahoo, with new 'vision,' set to report earnings
STORY Lobbyists go to battle over spectrum
STORY Dell halts the sale of WebPC line

Marcus C. Thomas

From: [redacted]
To: [redacted] Ed Allen <eallen@fbi.gov>; Marcus [redacted] <mthomas@ibiacademy.edu> [redacted]
Sent: Tuesday, July 11, 2000 10:05 AM
Subject: Carnivore article .... !!

All FYI ... if you are not already aware !!! Source is UK ZDnet page !!

[redacted]

News Burst: FBI uses covert email surveillance system

Tue, 11 Jul 2000 16:21:36 GMT

Will Knight

A super-fast scanning system nicknamed 'Carnivore' is being used by the FBI to covertly search through email messages, says the Wall Street Journal

America's Federal Bureau of Investigation (FBI) is using a super-fast email scanning system dubbed "Carnivore" to covertly trawl through email messages in order to capture suspected criminals, reports the Wall Street Journal Tuesday.

The revelations have caused a furore among privacy and security advocates, because it requires a direct connection to a commercial ISP's network, giving the authorities, in theory, access to all Internet communications.

Carnivore is reportedly nothing more than a personal computer fitted with special software capable of scanning millions of emails in a second.

According to the WSJ's report Carnivore, which was launched last year, has been used to gather evidence in fewer than 100 criminal cases.

Doc #12

07/11/2000

FBI e-mail Snooping Device Attacked

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - Civil liberties and privacy groups are railing against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.

The system, called ``Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.

When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.

Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

``Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target,'' read the letter. ``This 'trust us, we are the government' approach is the antithesis of the procedures required under our wiretapping laws.''

Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping data-tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, are already intrusive.

``Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target,'' Steinhardt said in an interview. ``When conducting these kinds of investigations, the information should be restricted to only addressing information.''

A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the House Judiciary subcommittee on the Constitution, said the congressman had no comment on the letter.

In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law firm in Washington, said he represented an Internet provider that refused to install the Carnivore system. The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared suits from customers unhappy with the government looking into all

DOC #13

the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents," Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost its court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said the main problem with Carnivore is its mystery.

``The FBI is placing a black box inside the computer network of an ISP," Dempsey said. ``Not even the ISP knows exactly what that gizmo is doing."

But Dempsey said Internet providers contributed to the problem, by saying that current technology does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

``The service providers said they didn't know how to comply with court orders," Dempsey said. ``By taking that position, they have hurt themselves, putting themselves into a box."

Marcus Thomas, who heads the FBI's cybertechnology section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

``This is just a specialized sniffer," Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, and it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely - show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

``The FBI should make this gizmo an open-source product," he said. ``Then the secret is gone."

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

American Civil Liberties Union: http://www.aclu.org

Center for Democracy and Technology: http://www.cdt.org

Pretty Good Privacy (PGP): www.pgp.com

AP-NY-07-12-00 0812EDT

Copyright 2000 The Associated Press.

washingtonpost.com Home | Register Web Search:

The Washington Post ONLINE

7% Bonus Furniture Discount

Need internet access for your office?

Quick Quotes: Enter symbols separated by a space (Get Quotes)

Look Up Symbols | Portfolio | Index

News Home Page
News Digest
OnPolitics
Nation
World
Metro
Business/Tech
Market News
Portfolio
Technology
Company Research
Mutual Funds
Personal Finance
Industries
Columnists
Special Reports
Live Online
Real Estate
Business/Tech Index
Sports
Style
Education
Travel
Health
Opinion
Weather
Weekly Sections
Classifieds
Print Edition
Archives
News Index
Help

Partners: BRITANNICA.COM

FBI's Internet Wiretaps Raise Privacy Concerns

By John Schwartz
Washington Post Staff Writer
Tuesday, July 11, 2000; Page A01

• Privacy Special Report
• What's Your Opinion?
E-Mail This Article
Printer-Friendly Version

The FBI has deployed an automated system to wiretap the Internet, giving authorities a new tool to police cyberspace but drawing concerns among civil libertarians and privacy advocates about how it might be used.

The new computer system, dubbed "Carnivore" inside the FBI because it rapidly finds the "meat" in vast amounts of data, was developed at FBI computer labs in Quantico, Va., and has been used in fewer than 50 cases so far.

But that number is sure to rise, said Marcus Thomas, chief of the FBI's cyber-technology section at Quantico. "In criminal situations there's not yet been a large call for it," he said, but the bureau already has seen "growth in the rate of requests."

Civil liberties groups said the new system raises troubling issues about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, the new technology also could scan private information about legal activities.

"It goes to the heart of how the Fourth Amendment and the federal wiretap statute are going to be applied in the Internet age," said Marc Rotenberg, head of the Washington-based Electronic Privacy Information Center.

The new system, which operates on off-the-shelf personal computers, takes advantage of one of the fundamental principles of the Internet: that virtually all such communications are broken up into "packets," or uniform chunks of data. Computers on the Internet break up e-mail messages, World Wide Web site traffic and other information into pieces and route the packets across the global network, where they are reassembled on the other end.

FBI programmers devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

Shop
$296
3COM Palm Organ
Send

Se
N
P
Ad

Prin New Coun Land Calls Risk' Post.
Truc Amo Homi Coun Washi 07/09/

More New

Nee ac yo

The ability to distinguish between packets allows law enforcement officials to tailor their searches so that, for example, they can examine e-mail but leave alone a suspect's online shopping activities. The system could be tuned to do as little as monitoring how many e-mail messages the suspect sends and to whom they are addressed--the equivalent of a telephone "pen register," which takes down telephone numbers being called without grabbing the content of those calls.

"That's the good news," said James Dempsey, an analyst with the Center for Democracy and Technology, a Washington high-tech policy group. "It is a more discriminating device" than a full wiretap, he said.

But Dempsey expressed worries about the new system, which would be installed at the offices of a suspect's Internet service provider. Just as the device could be used to fine-tune a search, it also could used for broad sweeps of data. "The bad news is that it's a black box the government wants to insert into the premises of a service provider. Nobody knows that it does what the government claims it would do," Dempsey said.

Existence of the Carnivore system was discussed in a Wall Street Journal article yesterday, which reported that the FBI showed the system to telecommunications industry experts two weeks ago.

Albert Gidari, a lawyer who works for the wireless industry, was present at the FBI demonstration. He said the FBI's announcement was intended to counter industry assertions that it would be very difficult to provide the kind of pen-register wiretap capability that the agency wants.

Since the demonstration, Gidari said, one faction within telecommunications industry was pleased with the FBI's efforts. But Gidari said the other faction was saying: "Wait a minute--what are the liability issues? What are the privacy issues? We don't want third-party software on our system."

Although Congress has passed legislation requiring telephone companies to make their developing high-tech networks easy to wiretap, Gidari is one of a large number of industry experts who believe the law does not apply to wiretapping the Internet. "The FBI overreaches in everything they do," said Gidari, who is president of G-Savvy, an Internet consulting company.

A former federal prosecutor sounded a more supportive tone. "If what it does is it helps comply with wiretaps, and it helps minimize what you're getting--to help get what the court authorizes you to get--there's nothing wrong with it," said Mark Rasch, now a security consultant with Reston-based Global Integrity.

Still, Rasch said the technology raised questions that have yet to be fully explored by law enforcement. The PC robocop examines all packets coming through a computer network but gives live law enforcement officers only those packets related to the subject of the investigation.

"The stuff that is examined only by a computer and not by a human being--was that information searched?" Rasch asked. He then suggested

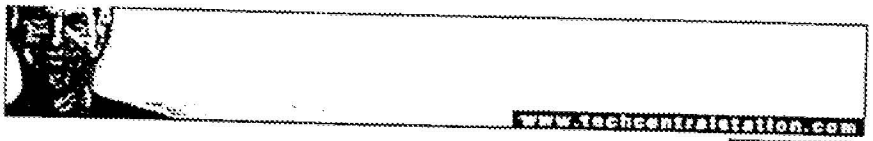
an answer: "It is a search, but it is to an extent less invasive than it would be if you did not use this technology."

The first news of Carnivore actually came in April during congressional testimony by Washington lawyer Robert Corn-Revere, who represented an Internet service provider that tried to resist attaching the system to its network. Corn-Revere suggested that such a system could be used to track dissidents and journalists online. "There are some human rights issues here," he said.

But Thomas of the FBI said there is nothing mysterious about the new device. "This is an effort on the FBI's part to keep pace with changes in technology--to maintain our ability" to lawfully intercept everything from pen-register data to full wiretaps with court authorization. "It's not an increase in our authority; it doesn't present a change of volume in what we do," he said.

© 2000 The Washington Post Company

◀ Previous Article Back to the top Next Article ▶



OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #4, OGC/TECHNOLOGY LAW UNIT FILE (PGS. 162 + 163)

_____ Page(s) withheld for the following reason(s): _____

_____

_____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #15, PGS. 1+2 (Pages 636-637)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Get credit for that old IBM PC, laptop

BY PAULA SHAKI TRIMBLE

Federal agencies will be able to obtain credit toward the purchase of new IBM Corp. PCs and laptops by donating their old computers to charity via a unique governmentwide contract.

The Department of Veterans Affairs Special Services office and the Air Force Medical Logistics Office awarded a decentralized blanket purchase agreement last week to iGov.com, an online computer equipment reseller, that would allow government customers to receive a trade-in allowance for their older IBM equipment at the time of purchase.

Agencies could receive a $300 credit for IBM PCs that have 486 or faster processors and are Year 2000-compliant, said Corinne Lingebach, iGov.com's program manager for the Technical Refresh and Trade-In program, which is open to all government agencies and runs through Oct. 8, 2002. The credit can be applied to the purchase of a new computer. Agencies could receive a $500 credit for each laptop turned in.

The BPA, based on iGov.com's General Services Administration schedule contract, "is a better value, and it enhances programs we already have," said government contracting officer Mary Rust. "Only iGov offers the trade-in, so it's unique."

The contract guarantees iGov.com at least $500,000 in sales, but the company anticipates more than $25 million in sales over the life of the contract, said Brad Mack, iGov.com's vice president of sales.

In the future, Rust hopes to add other types of computer equipment to the program. Although there are no other contracts that offer trade-in credits, Rust's office does offer other unique programs that benefit schools and other charities.

iGov.com partnered with Gifts In Kind International, an Alexandria, Va.-based charity organization, to refurbish federal agencies' obsolete systems and deliver them to charitable organizations.

Agencies can specify a charity or allow Gifts In Kind to choose the charity that will receive the computer. Gifts In Kind's Recycle Technology program, which supplies refurbished computers to needy organizations, has donated about 20,000 computers a year to nonprofit organizations since it started in 1994, said Doug McAllister, Gifts In Kind's director of marketing and communications. "Computers and technology are high on the needs list for charity," McAllister said.

Responsibility for deleting classified information from computer hard drives or removing the hard drives themselves rests with the agency trading in the equipment, Mack said. ■

ACLU: Block FBI e-snoops

BY DAN VERTON

The American Civil Liberties Union appealed to Congress last week to protect Americans from unreasonable searches and seizures on the Internet in light of recent revelations that a new monitoring tool could enable the FBI to intercept the e-mail of law-abiding citizens.



In a letter to the House Judiciary Committee's Constitution Subcommitte, ACLU director Laura Murphy argued that the FBI's new Carnivore e-mail surveillance system gives federal law enforcement officers access to the e-mail of every customer of an Internet service provider and the e-mail of every person who communicates with them.

"The Carnivore system gives law enforcement e-mail interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act" in 1986, Murphy stated in the letter. "The ACLU urges the subcommittee to accelerate its consideration of the application of the Fourth Amendment in the Digital Age."

The Fourth Amendment to the Constitution protects the public from unreasonable searches and seizures.

Attorney General Janet Reno said July 13 that she is now looking into the allegations. "When we develop new technology, when we apply the Constitution, I want to make sure that we apply it in a consistent and balanced way," Reno said.

Robert Corn-Revere, an Internet and communications lawyer with the Washington, D.C.-based law firm Hogan & Hartson LLP, first divulged evidence of the Carnivore system's abilities during a congressional hearing in April. The FBI must have a court order to use Carnivore.

Once approved, Carnivore is attached directly to an ISP's network and gives the FBI access to all e-mail traffic flowing across the network, according to the ACLU. The ACLU and others have raised concerns that Carnivore intercepts information from the headers of e-mail messages and may divulge details about the contents of the messages.

"The FBI and the law enforcement and national security communities in general are offering a trade: less privacy due to increased use of technology in surveillance in return for greater safety for the public," said Daniel Ryan, a lawyer and former director of Information Systems Security at the Pentagon. ■

5/24/02 Release - Page 638

Intell turf battles rage

BY DAN VERTON

Major portions of a bill that would authorize appropriations for the U.S. intelligence community would significantly limit the Defense Department's ability to support military operations, warn Defense Secretary William Cohen and his top military adviser.



William Cohen, Secretary of Defense

Cohen and Army Gen. Henry Shelton, chairman of the Joint Chiefs of Staff, recently sent a letter to senior lawmakers on Capitol Hill protesting a proposal by the House Permanent Select Committee on Intelligence to establish an intelligence community communications architect position within the CIA. The chief architect would have broad responsibilities for the development of a worldwide telecommunications system that would serve the intelligence community, the bulk of which now resides in DOD and not the CIA.

The chief architect, supported by a 30-person staff, would be funded with $80 million in start-up money taken directly from the budgets of the Pentagon's National Reconnaissance Office, the National Security Agency and the Defense Intelligence Agency, according to the bill.

"This unilateral and independent architectural office would seriously damage, if not totally destroy, the efforts of the DOD chief information officer, who has ongoing activities with the [intelligence community] and Defense intelligence component CIOs to advance interoperability between and among intelligence producers and consumers," Cohen and Shelton told Congress. The House Armed Services Committee included Cohen and Shelton's letter in a report on the fiscal 2001 Intelligence Authorization bill, released last month.

But the Pentagon is also concerned about the impact the new office might have on DOD's efforts to orchestrate a Global Information Grid (GIG), according to the Cohen and Shelton letter. The Pentagon has been working on the GIG concept for more than a year and envisions a global network capable of delivering secure information to all users.

The GIG architecture "puts a premium on the assured and timely access by our warfighters and policy-makers to all forms of information, including intelligence," a Pentagon spokesperson said. However, "there shouldn't be separate architectures for combat functions, for support functions [or] for intelligence functions. Otherwise, we're back at the stovepiped, stand-alone systems that don't talk to one another in a timely fashion."

An official from the Pentagon's office of Command, Control, Communications and Intelligence also said that the Pentagon supports a broader GIG concept as opposed to a narrow, intelligence-only communications architecture.

"Solutions which take down the old barriers to interoperability and harness our collaborative networking and computing capabilities have the most value and are deserving of support," the official said. "Our concerns with the proposed intelligence communications architect are lessened by the extent to which that entity is free to support the broader Global Information Grid architecture in preference to a narrower, intelligence-only network."

Cohen and Shelton expressed opposition to Congress' proposal to expedite the real-world use of the Joint Intelligence Virtual Architecture tool in the intelligence community, saying it is "premature" to designate the software capability as the community standard for collaboration. The program is a next-generation digital collaboration effort headed up by Defense Intelligence Agency. Congress called for oversight of the program to be transferred from DOD to the CIA.

"We feel strongly that it would be counterproductive both to prohibit further non-JIVA technology pursuits and to remove the program from the DOD oversight that has made it the success that the committee commends," stated Cohen and Shelton.

The CIA declined to comment on the proposed legislation. ■

A WAR, NOT A BATTLE

Intelligence experts characterized the latest report on the bill from the House Armed Services Committee as little more than a tool in the struggle for control over the intelligence budget between the House and the Senate Select Committee on Intelligence, chaired by Sen. Richard Shelby (R-Ala.).

Others said the debate centers on the larger questions of reforming the intelligence community and who should be in charge.

"It's just one more instance of the turf battle over intelligence," said Steven Aftergood, an intelligence specialist with the Federation of American Scientists. "The basic question is, will there be a strong director of central intelligence who is in charge of the whole community? The Defense Department says no."

Furthermore, "because of the ongoing militarization of intelligence, my bet is that the Pentagon will get its way," he said.

Robert Steele, a 25-year veteran of the intelligence community and author of the recent book "On Intelligence: Spies and Secrecy in an Open World," said the Information Age has challenged the whole notion of having a central agency responsible for intelligence. "In the age of distributed information, the concept of central intelligence is an oxymoron," Steele said.

– Dan Verton

PHOTO/AP

5/24/02 Release - Page 629

YAHOO! NEWS Home - Yahoo! - My Yahoo! - News Alerts - Help AP Assoc Press

Yahoo! Platinum Visa : 2.9% APR ~ Instant Credit ~ Rewards with GiftCertificates.com ~ No Annual Fee.

Home Top Stories Business Tech Politics World Local Entertainment Sports Science Health Full Coverag

Politics News - updated 7:17 AM ET Jul 12 Add to My Yaho

Reuters | AP | Elections | ABCNews

Tuesday July 11 7:26 PM ET

FBI e-mail Snooping Device Attacked

By D. IAN HOPPER, Associated Press Writer

Speak your mind
Discuss this story with other people.
[Start a Conversation]
(Requires Yahoo! Messenger)

WASHINGTON (AP) - Civil liberties and privacy groups railed Tuesday against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.

The system, called ``Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.

When Carnivore is placed at an Internet Service Provider, it scans all incoming and outgoing e-mails f messages associated with the target of a criminal probe.

In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.

Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

``Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations the specified target," read the letter. ``This 'trust us, we are the government' approach is the antithesis o the procedures required under our wiretapping laws."

Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping dat tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, is already intrusive.

"Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target," Steinhardt said in an interview. ``When conductin these kinds of investigations, the information should be restricted to only addressing information."

A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the Constitution subcommittee, said that the congressman had no immediate comment on the letter.

Doc. #16

In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law fir in Washington, said that he represented an Internet provider that refused to install the Carnivore syste The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared sui from customers unhappy with the government looking in to all the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents,'' Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost their court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said that the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said that the main problem with Carnivore is it's mystery.

``The FBI is placing a black box inside the computer network of an ISP,'' Dempsey said. ``Not even th ISP knows exactly what that gizmo is doing.''

But Dempsey said that Internet providers contributed to the problem, by saying that current technolog does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

``The service providers said they didn't know how to comply with court orders,'' Dempsey said. ``By taking that position, they have hurt themselves, putting themselves into a box.''

Marcus Thomas, who heads the FBI's Cyber Technology Section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

``This is just a specialized sniffer,'' Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, an it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely - show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

``The FBI should make this gizmo an open-source product,'' he said. ``Then the secret is gone.''

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

American Civil Liberties Union: http://www.aclu.org

Center for Democracy and Technology: http://www.cdt.org

Pretty Good Privacy (PGP): www.pgp.com

Email this story - (View most popular) | Printer-friendly format

Archived Stories by Date: Jul 11 Go

Search News

Search Advanced

Search: Stories Photos Full Coverage

Home Top Stories Business Tech Politics World Local Entertainment Sports Science Health Full Coverag

Questions or Comments

Copyright © 2000 The Associated Press. All rights reserved.
The information contained in the AP News report may not be published, broadcast, rewritten or redistributed without the prior written authority of The Associated Press.

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☒ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: _____
Sender's Initials: _____
Number of Pages: _____
(including cover sheet)

To: _____ Date: 7/12/00
Name of Office

Facsimile Number: 703-632-6081

Attn: MARCUS Thomas
Name Room Telephone

From: CIS
Name of Office

Subject: _____

Special Handling Instructions: _____

Originator's Name: [redacted] Telephone: 6C-1 / 67C-1

Originator's Facsimile Number: _____

Approved: _____

Brief Description of Communication Faxed: FYI.

WARNING

5/24/02 Release - Page 643

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

Doc #17

Reno to review the FBI's Internet wiretap system

WASHINGTON, July 13 (Reuters) - U.S. Attorney General Janet Reno said on Thursday she would review a new FBI automated computer system that can wiretap the Internet to determine whether it might infringe on privacy rights.

``I'm taking a look at it now to make sure that we balance the rights of all Americans with the technology of today," Reno said when asked about the FBI system known as ``Carnivore" that can be used to monitor all e-mails of a criminal suspect.

Reno emphasised that any such wiretaps, which are placed on an Internet service provider's system, cannot be be done without an appropriate court order ``according to processes and procedures used now for lawful surveillance."

``We are looking at it to see what is needed, if anything," she said. ``If additional regulations are needed, we will pursue those."

She told her weekly news briefing that she wanted to make sure that the new technology does not become ``a cause of concern for privacy interests."

The American Civil Liberties Union (ACLU) and other privacy advocates have expressed concern the new system could scan private information about legal activities, resulting in excessive monitoring of online communications. Besides e-mails, the system can monitor visits to Web sites and Internet chat sessions.

Reno said she only began looking into the issue and asking questions after news articles appeared earlier this week. The FBI recently demonstrated the system to executives in the telecommunications industry.

``We have known about the capacity to do this. Its application and what has been done had not been brought to my attention," Reno said.

The FBI's director, Louis Freeh, reports to Reno.

``I just want to make sure that industry, privacy interests, law enforcement interests are all fully advised so that we can consider anybody's concerns and make sure that we address them," Reno said.

She was unable to say whether the system would continue to operate until her review was underway.

13:29 07-13-00

Copyright 2000 Reuters Limited. All rights reserved.

Doc. #18

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of DOC. #12, OGC/TECHNOLOGY LAW UNIT FILE (PAGES 268-270)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #19 (Pages 647-649)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

washingtonpost.com Home | Register Web Search: GO

The Washington Post ONLINE



PERSONAL CO

Quick Quotes: Enter symbols separated by a space Get Quotes
Look Up Symbols | Portfolio | Index



News Home Page
News Digest
OnPolitics
Nation
World
Metro
Business/Tech
Market News
Portfolio
Technology
Company Research
Mutual Funds
Personal Finance
Industries
Columnists
Special Reports
Live Online
Real Estate
Business/Tech Index
Sports
Style
Education
Travel
Health
Opinion
Weather
Weekly Sections
Classifieds
Print Edition
Archives
News Index
Help

Britannica.com

Controls on Export of Encryption Software to be Eased

By John Schwartz
Washington Post Staff Writer
Monday, July 17, 2000; 1:12 PM

The Clinton administration announced today that it will loosen controls on the export of encryption software -- the programs that help users scramble messages and data to protect it from prying eyes -- and called for new legislation intended to make sense of wiretapping in the Internet age.

"We need to seek a better balance amongst the sometimes competing goals of the protection of public safety, the achievement of economic growth and digital opportunity -- and the preservation of privacy and civil liberties," said White House Chief of Staff John Podesta in a speech delivered today at the National Press Club.

Under the new policy, American companies will be able to export the strongest cryptography products to users in any nation in the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The government will eliminate a current statutory 30-day waiting period before such exports can take place, but keeps in place a requirement that new technologies be submitted to the government for a technical review.

Encryption has been a high-tech battlefield from the early days of the Clinton administration. Few technologies are as important in the fight to maintain personal and business privacy -- but few technologies, as well, present such daunting issues for law enforcement, which warns that criminals and terrorists can use "crypto" to cloak their plans and activities. But high-tech companies successfully argued that U.S. restrictions only harmed American companies, since overseas firms were successfully marketing strong encryption products, and in January the Clinton administration reduced controls on encryption exports. In

Live Online

- Protect Your Identity: David Steer of TRUSTe discusses how to protect sensitive personal information at 11 a.m. Wednesday.
- Protect Your Kids: Amy Aidman of the Center for Media Education discusses ways to protect you children online at 1 p.m. Thursday.

Special Report

Privacy

What's Your Opinion?
E-Mail This Article
Printer-Friendly Version

Shopping
J.K. Rowling
Browse through he at the Auth Bookshelf
Hallmark

Search
News
Post A
Advance

Related
Your PC I Watching Washingto 07/14/00)
FBI's Intr Wiretaps Privacy C (The Washi Post, 07/12
FTC Sues Store Ove Sell Data Washingto 07/11/00)
U.S. to En On Expor Secrecy S (The Washi Post, 09/17

From Bri Understa Data Encr

Need h

the Clinton administration reduced controls on encryption exports. In today's speech, Podesta stressed the now-familiar theme that the online revolution has been a mixed blessing. At the same time that the Internet makes Shakespearean sonnets and new photos of Mars available anywhere in the world, it has undermined the pirvacy of our most sensitive financial and medical records, and allows such evildoers as international drug trafffickers to communicate freely and secretly.

"That's why we have to make sure the Internet is used to the benefit of people – not to their detriment," the Podesta said.

The most sweeping part of the Podesta address was a call for a thorough rethinking of the Fourth Amendment's protection against unreasonable search and seizure in the Internet age. Electronic mail transmitted by high-speed connections such as DSL modems, Podesta's speech argued, has never enjoyed the legal protections the law gives to telephone conversations – or to slower dial-up modems under the Electronic Privacy Communications Act of 1984. At the same time, cable privacy laws are tougher than wiretap standards when it comes to gaining access to subscriber records – which could include e-mail sent via cable modem. Podesta called for new legislation to address the inconsistencies in the legal framework. "It's time to adopt legislative protections that map these important privacy principles onto the latest technology," he said.

Podesta's speech also make oblique reference to a controversial new surveillance technology revealed last week, which is known as "Carnivore." Carnivore gives government the ability to selectively monitor Internet traffic of individuals in ways that can give law enforcement the Internet equivalent of "trap and trace" capabilities used in telephone surveillance. Unlike full-fledged wiretaps, the judicial oversight of trap and trace is slight, and the protection against abuses of the technology by law enforcement is weak. Podesta called for "greater judicial oversight of trap and trace authorities."

Podesta's speech stated that this legislation could be passed by the end of the year – an unlikely prospect in these waning days of the legislative session. "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," he said.

The speech also made the point that the administration's preference is for public-private partnerships to make the Internet secure against attack, but noted that Congress has not appropriated any of the $90 million President Clinton has requested for security research and cyber policing. "It's time," Podesta noted, that "they picked up the pace and provided the protections that are essential to America's cyber security.,"

The speech was not well received by civil liberties advocates, who have fought Carnivore and other administration attempts to develop wiretapping capabilities on the Internet. Barry Steinhardt, associate director of the American Civil Liberties Union, called the speech

"deeply disappointing."

Rather than defending Carnivore, Steinhardt said, Podesta should have announced that the administration was suspending its use. "Carnivore represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic," Steinhardt said in a statement.

"While the Clinton administration's proposals have some heartening qualities to them, they are too little and too late," with too little time in the legislative session to pass new bills. "Last-minute legislative proposals cannot satisfy the deep privacy concerns of the American public," Steinhardt said.

© 2000 The Washington Post Company

◂ Previous Article Back to the top Next Article ▸



washingtonpost.com Home | Register Web Search: GO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

3 Page(s) withheld for the following reason(s): PREVIOUSLY RELEASED AS PART OF EC PACKET #5 (RELEASE #4)

☒ The following number is to be used for reference regarding these pages: DOCUMENT #21 (Pages 653-655)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Technology

The New York Times on the Web

Home | Site Index | Site Search | Forums | Archives | Marketplace

bizzed
POWERFUL E-PRODUCTS AND SERVICES TO HELP YOU ACHIEVE YOUR OWN VERSION OF SUCCESS.
What you do with bizzed is your business

July 18, 2000

Proposal Offers Surveillance Rules for the Internet

White House Tries to Balance Rights of Computer Users and Law Enforcement

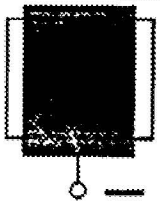
By STEPHEN LABATON with MATT RICHTEL

WASHINGTON, July 17 -- The White House said today that it would propose legislation to set legal requirements for surveillance in cyberspace by law enforcement authorities similar in some ways to those for telephone wiretaps.

Privacy advocates and civil liberties groups welcomed some aspects of the proposal but said they remained alarmed about a new F.B.I. computer system that searches and intercepts private e-mail and can easily capture communications of people not suspected of crimes.

The legislative proposal was made as the administration also announced today that it had eased export controls on encryption technology, making it significantly easier for American companies to sell software products to the European Union and eight other trading partners that can be used to keep computer data and communications secure.

Both the electronic surveillance proposal and the export control changes are part of a broader policy outlined in a speech today by John D. Podesta, the White House chief of staff. He said the policy tries to balance the privacy rights of computer users against the needs of law enforcement to be able to monitor digital communications.



NET PRIVACY

IN DEPTH
Privacy and the Internet

RECENT NEWS
Administration Retools Rules on Encryption (July 18, 2000)

Reno Says Review Is Under Way on Net 'Wiretapping' (July 14, 2000)

Administration Issues Privacy Directives (June 13, 2000)

FORUM
Can Privacy be Protected Online?

Go t
defin
and get
interact
to help
your fu
efficien
and effe

• Fund
Enter y
goals,
identifi
we beli

• Virtua
Learn h
more ir
investn

• My del
Custom
page to
the per
your fu

• Timely
Get det
pricing
informe
securiti
portfol

M
Salome
Pa
Morgan S

Define
A

5/24/02 Release - Page 656

DOC. #22

Congress and federal regulators have done little work in the area, even as the world has quickly come to rely heavily on communications through cyberspace. More than 1.4 billion e-mail messages change hands every day.

The administration's legislative proposal on electronic surveillance tries to fix the inconsistent patchwork of laws that apply different standards to telephone, cable and other technologies with a single standard for those systems and the Internet. Prospects for the proposal in Congress are uncertain.

Until now, law enforcement agencies have been able to monitor electronic communication with only modest court supervision.

The proposed legislation would require that the same standards that apply to the interception of the content of telephone calls apply to the interception of e-mail messages. Specifically, it would require law enforcement agents to demonstrate that they have probable cause of a crime to obtain a court order seeking the contents of a suspect's e-mail messages.

The proposal would also give federal magistrates greater authority to review requests by law enforcement authorities for so-called pen registers -- lists of the phone numbers called from a particular location and the time of the calls. The magistrates now have no authority to question the request for such lists, which are frequently used by the authorities.

In the context of the Internet, existing laws are ambiguous about what standards apply for different kinds of surveillance. Many limitations imposed on law enforcement in the context of telephone wiretaps -- like the requirement that such taps be approved at the highest level of the Justice Department -- do not appear to apply to e-mail surveillance.

Moreover, the Cable Act of 1984 sets a far harder burden for government agents to satisfy when trying to monitor computers using cable modems than when monitoring telephones. That has proved troublesome for law enforcement authorities as more Americans begin to use high-speed Internet service through cable networks. The Cable Act also requires that the target of the surveillance be given notice and an opportunity to challenge the request.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Mr. Podesta said in a speech at the National Press Club. "Our proposed legislation would harmonize the legal standards that apply to law enforcement's access to e-mails, telephone calls and cable services."

White House officials said today that they hoped the proposal would break a logjam in Congress where a variety of different measures have been introduced dealing with electronic surveillance. The

administration's proposal adopts some elements of both Democratic and Republican bills.

But Congressional aides said there was too little time left in the legislative session and that the matter would in all likelihood remain unresolved until after the next term begins, in 2001.

Administration officials said the proposal would apply to communications that either begin or end in the United States. It would not apply to e-mail messages transmitted entirely outside the country.

Privacy and civil liberties groups criticized the administration's proposal because it would continue to permit the government to use a new surveillance system that the groups say may be used far more broadly than older technologies, enabling federal agents to monitor an unlimited amount of innocent communications, including those of people who are not targets of criminal investigations.

The system, used by the Federal Bureau of Investigation, is called Carnivore, so named, agents say, because it is able to quickly get the "meat" in huge quantities of e-mail messages, so-called instant messaging and other communications between computers.

Carnivore is housed in a small black box and consists of hardware and software that trolls for information after being connected to the network of an Internet service provider. Once installed, it has the ability to monitor all of the e-mail on a network, from the list of what mail is sent to the actual content of the communications.

Marcus C. Thomas, section chief of the Cyber Technology Section of the F.B.I., said the technology was developed 18 months ago by F.B.I. engineers and has been used fewer than 25 times. Mr. Thomas said that Carnivore had potentially broad capabilities and that he understood the concerns of privacy groups.

"It can do a ton of things," he said. "That's why it's illegal to do so without a clear order from the court."

He said that most Internet service providers had cooperated with requests to use Carnivore.

Privacy groups and some Internet service providers have been deeply critical of the use of Carnivore because, once installed on a network, it permits the government to take whatever information it wants.

Moreover, the government has not said what it does with the extraneous material it gathers that is not relevant to the particular surveillance.

The issue does not often arise today with the monitoring of telephone conversations because when a law enforcement authority wants to see a list of telephone calls made by a suspect, the agent

gets an order from a magistrate, presents the order to a telephone company, and the company then turns over the list.

In at least one instance, an Internet company did not cooperate so readily with the government. In December, federal marshals approached the company with a court order permitting them to deploy a device to register time, date and source information involving e-mail messages sent to and from a specified account.

Trying to establish a single standard for different technologies.

Concerned the device would record broader information, the company countered with a compromise: it would provide the government with the requested information about e-mail senders and recipients, according to Robert Corn-Revere, a lawyer for the company, in recent Congressional testimony. The company was later identified as EarthLink, a service provider with 3.5 million subscribers.

Mr. Corn-Revere said the government initially accepted the compromise but later became dissatisfied and wished to use its own device. EarthLink objected but was overruled by a a federal court, which ordered the device deployed.

Other Internet companies have also been critical of Carnivore.

William L. Schrader, chairman and chief executive of PSINet, a major commercial Internet service provider, said that the system gave the F.B.I. the ability to monitor e-mail messages of every person on a given network. He said he would refuse to permit the government to use the technology at PSINet unless agents could prove that it could only sift out the traffic from a given individual that is the target of a court order.

"I object to American citizens and any citizens of the world always being subject to someone monitoring their e-mail," said Mr. Schrader, whose company serves about 100,000 businesses and more than 10 million users. "I believe it's unconstitutional and I'll wait for the Supreme Court to force me to do it."

Civil liberties groups, meanwhile, said that today's policy announcement was an inadequate response to the growing controversy over the deployment of Carnivore.

"Today's speech was camouflage to cover the mess that is Carnivore," said Barry Steinhardt, an associate director of the American Civil Liberties Union. "In light of the public and Congressional criticism of Carnivore, we had hoped and expected far more from an administration that likes to tout its sensitivity to privacy rights. Rather than glossing over Carnivore, Podesta should have announced that the administration was suspending its use."

Facing growing concerns about

Concern that the proposals allow federal agents too much leeway.

Facing growing concerns about Carnivore, Attorney General Janet Reno said on Thursday that she would review whether the system was being used in a manner consistent with privacy rights in the Constitution and in federal law. A subcommittee of the House is set to hold a hearing next week on the system.

While the civil liberties and privacy groups applauded giving judges greater discretion to review certain kinds of requests for surveillance, they were critical of other aspects of the proposal.

Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology, criticized the administration for lowering the standards for surveillance of cable modems rather than raising the standards for telephone surveillance.

"The Cable Act provides for one of the best privacy protections in the United States," Mr. Rotenberg said. "The question is whether to harmonize up or harmonize down. Our view is this harmonizes down."

But administration officials said the Cable Act never contemplated that there would be broad use of cable modems for e-mail traffic and that the standards used for obtaining warrants for telephone surveillance should also apply to digital communications through cable networks.

Ask Technology questions in Abuzz, a new knowledge network from The New York Times. Get answers and tell other readers what you know.

abuzz



Copyright 2000 The New York Times Company

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #10, OGC FRONT OFFICE FILE (PGS. 16 + 17)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #23 (Pages 661-662)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Copyright 2000 U.P.I.
United Press International

July 21, 2000, Friday 01:27 PM Eastern Time

SECTION: GENERAL NEWS

LENGTH: 713 words

HEADLINE: The FBI's **Carnivore:** It bites only under court order

BYLINE: By MICHAEL KIRKLAND

DATELINE: WASHINGTON, July 21

BODY:
The FBI is in a full-court press to reassure the public about its **Carnivore** intercept system, designed to perform a "wire-tapping" function on the Internet.

During a background briefing for reporters Friday, FBI officials said the system can only be used under court order, and that "procedure, training and audits" of its use will prevent technicians from attempting unauthorized snooping.

A senior official added that the bureau is looking for "a couple of technical institutions" outside the FBI to independently "validate and evaluate" the system's operation and integrity.

The system has drawn fire from an unlikely coalition of critics.

The American Civil Liberties Union and similar groups have attacked **Carnivore** as new government intrusion without proper safeguards. The Republican leadership of Congress has also been highly critical, and a House Judiciary subcommittee has planned hearings Monday to explore what some politicians believe is a need for new federal restrictions on its use.

Meanwhile, the average computer user may feel that Big Brother is looking over his or her shoulder.

Not so, says the FBI in its most soothing official voice.

At Friday's briefing in a conference room at bureau headquarters in Washington, the senior FBI official said the **Carnivore** program is three years old, and, "It began because we were receiving court orders to do intercepts on the Internet."

Carnivore software - so named because it looks for the "meat" in a data stream - uses a Windows platform and is contained on a personal computer that is plugged into an Internet service provider. The access is allowed only for the length of time set out in a court order. "When the order expires, we take our equipment away," the senior official said.

The ISP usually performs some "pre-filtering" of data so that the amount of information traveling through the **Carnivore** "filter" is not overwhelming. The **Carnivore** device can perform a traditional "pen register" function on the Internet - record and store the origin and destination of e-mail - or capture the content of an e-mail message, much like a traditional phone tap, only in a much more specific way.

"That filter is configured to fit the contour of the court order we're assigned to do," the senior official said. In other words, it will only select and copy specific information authorized by a federal judge. The system targets e-mail by an "authorization" code peculiar to an individual user, and the FBI will not monitor subject lines on e-mail.

The filtering process will not slow down computer response time, another FBI official familiar with the technology said. "It's just passively watching the bits."

5/24/02 Release - Page 66
Doc. #24

The approval process for a **Carnivore** intercept is also extremely rigorous, an FBI official expert in cyber legal issues said. Investigators seeking a court order to use **Carnivore** must go through an internal FBI review process, then the request must be approved by the attorney general or the deputy attorney general before a federal judge is approached for a court order.

Less than a dozen such requests have been made over the last year for criminal probes - as opposed to national security investigations - and no request has been refused by a judge.

"These (intercepts) are not implemented trivially," the FBI legal official said, both because of the expense and the depth of review.

What about someone outside the FBI hacking into the **Carnivore** device and accessing an innocent person's e-mail?

"The device cannot be penetrated from the Internet side," the FBI technical official said. "Theoretically," a hacker could beat very high odds and randomly dial into a separate monitoring line, he added, but even that line is protected by heavy security.

The senior official at Friday's briefing conceded that the name of the system - **Carnivore** - has caused some apprehension. "Naming is always a very sensitive thing," the official said. "This experience is sobering." The official said the FBI would give some thought in the future to the effect the name of an operation or procedure might have on the public.

"Sniffer" might be a fairer term. "It's a customized packet sniffer," the FBI technical official said.

"A very well-focused sniffer," the senior official added.

LANGUAGE: ENGLISH

LOAD-DATE: July 21, 2000

FOCUS™
Search: General News;Carnivore

To narrow this search, please enter a word or phrase:

FOCUS

Example: **House of Representatives**

About LEXIS-NEXIS | Terms and Conditions | What's New
Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

10 Pages were not considered for release as they are duplicative of DOC. #13, OGC FRONT OFFICE FILE, PGS 15-25

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #25 (Pages 665 - 674)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

5 Pages were not considered for release as they are duplicative of DOC. #20, OPCA FILE (PGS. 514-518)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #26 (Pages 675-679)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

NewsMax.com

Controversy
Boortz on Boortz

NewsMax Home Page	Free E-mail News Alerts	Columnists	News Links	Late Night Jokes	Archives
Shopping Mall	Cartoons	Magazines Really Cheap	Forum	Classifieds	Contact Us



Advertise Your Banner Here

The Feds Can Read Your E-Mail

NewsMax.com
Wednesday, July 12, 2000

First it was Echelon, the global eavesdropping system Uncle Sam and John Bull have been using to spy on satellite-transmitted phone calls, e-mails and fax messages. Now it's Carnivore, the FBI's newest electronic snooping device that can read your e-mail right off your mail server.

Capable of scanning millions of e-mails a second, Carnivore can easily be used to monitor everybody's e-mail messages and transactions, including banking and Internet commerce. If they want to, the feds can find out what books you're buying online, what kind of banking transactions you conduct – in short, everything you do when you go online and send e-mail, whether private or commercial.

The FBI has been quietly monitoring e-mail for about a year. Two weeks ago the feds went public and explained the high-tech snooping operation to what the Wall Street Journal called "a roomful of astonished industry specialists."

According to the bureau, they've used Carnivore – so called because it can digest the "meat" of the information they're looking for – in less than 100 cases, in most cases to locate hackers but also to track terrorist and narcotics activities.

But there is nothing to stop Carnivore from making a meal of your e-mail messages and transactions if they decide that's what they want to do and can get a judge to issue a court order allowing them to tap your e-mail as they would your phones.

That's scant comfort considering the underhanded means the feds employed to get court orders to raid the Branch Davidian compound, or to win a judge's permission to stage what amounted to an illegal armed raid on Elian Gonzalez's Miami home.

Carnivore is nothing but a store-bought personal computer with special software that the FBI installs in the offices of Internet service providers (ISPs).

The computer is kept in a locked cage for about a month and a half. Every day

an agent comes by and retrieves the previous day's e-mail sent to or by someone suspected of a crime.

But critics say that Carnivore, like some ravening beast, is simply too hungry to be trusted – that it gives the feds far too much access to too much private information.

"This is more of a vacuum cleaner-type approach – it apparently rifles through everything," David Sobel, general counsel for the Electronic Privacy Information Center, told Fox News.

"It's potentially much more invasive than telephone surveillance."

Carnivore could conceivably monitor all the e-mail that moves through an ISP – not merely messages sent to or from the subject allegedly being monitored. Critics compare it to eavesdropping on all the phones in a neighborhood simply to zero in on just one phone.

Disturbingly, the FBI has prevailed in challenges against forcing ISPs to allow Carnivore to be installed in their offices. According to the Wall Street Journal, one unidentified ISP put up a legal fight against Carnivore early this year and lost.

The FBI defends Carnivore, insisting it is used selectively and monitors only the e-mail of the subject. They say that messages belonging to those not being probed, even if criminal, would not be admissible in court.

"The volume of e-mail in a location is generally fairly small and being managed by a small number of e-mail servers on a fairly low-speed network," said Marcus Thomas, chief of the FBI's cyber technology section.

"The system is not unlike 'sniffers' used within the networks every day."

That fails to satisfy critics such as Sobel. He says Carnivore is similar to Russia's surveillance system, called "SORM," which all Russian ISPs are forced to install to allow the government to spy on whomever it chooses.

It's also similar, he says, to the notorious Echelon, the National Security Agency's global eavesdropping system, which intercepts telecommunications transmissions from around the world and looks for keywords that could indicate illegal activity.

"Carnivore is really the latest indication of a very aggressive stance that the bureau is taking in collecting as much information as technically possible," Sobel said.

FBI spokesman Paul Bresson insists that law-abiding citizens have nothing to fear from Carnivore. "Anytime we develop a system, we're basically balancing the interests of national security against that of the privacy of the public," he said.

"This issue's always going to come up. We're always going to get questions. We understand that."

See articles on Echelon.

E-mail This Article to a Friend

Printer Friendly Version

E-mail a Comment to NewsMax.com Discuss this Article in NewsMax.com's Forum

Reprint Information

Home · Search · Free E-mail News · ZipMax.com-Free Webmail · Columnists · News Links · Late Night Jokes

Archives · Shopping Mall · Cartoons · Magazines · Forum · Classifieds · Contact Us

All Rights Reserved © NewsMax.com

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☒ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☒ Unclassified

Time Transmitted: 3:30 pm
Sender's Initials: slk
Number of Pages: 4
(including cover sheet)

To: Ed Allen
Name of Office

Date: 07/26/2000

Facsimile Number: 703-632-6081

Attn: _____
Name Room Telephone

From: FBI - San Diego
Name of Office

Subject: _____

Special Handling Instructions: _____

Originator's Name: SAC William D. Gore Telephone: 858-514-5600

Originator's Facsimile Number: 858-514-5890

Approved: WDG

Brief Description of Communication Faxed: _____

WARNING

Doc #28

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

5/24/02 Release

FD-350 (REV. 5-8-81)

MOUNT CLIPPING IN SPACE BELOW

The Eye of the FBI

Indicate page, newspaper, city, state
San Diego Union Tribune
San Diego, California

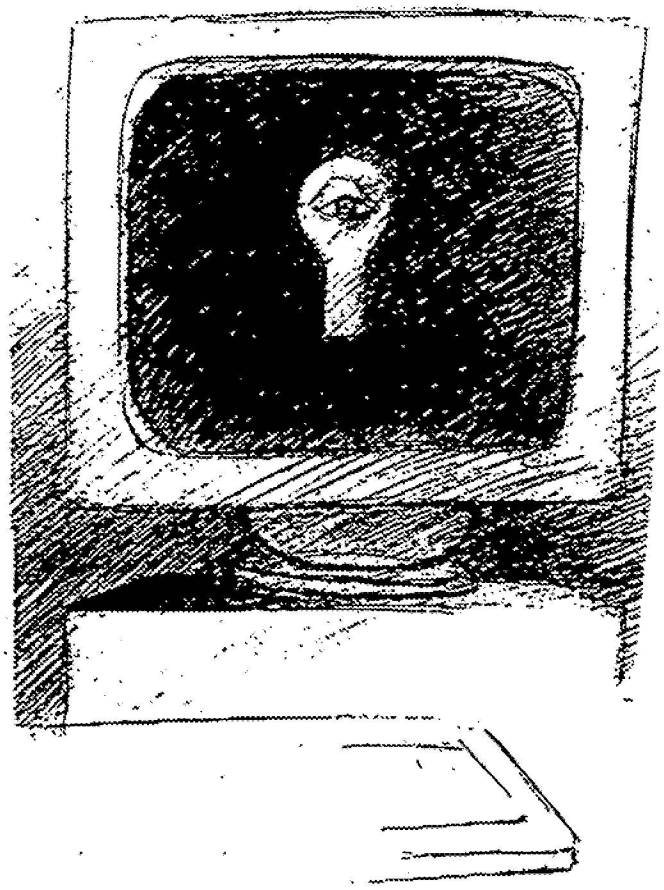
Page B-9

July 26, 2000

Title:
"The Eye of the FBI"

Submitting Office:
San Diego

Indexing:



Paul Tong

"Eye of the FBI" (continued)

By Lisa S. Dean

For those of you who thought that ECHELON, the multinational surveillance system, was a joke, here's something else for you to laugh at. It's a new system called "Carnivore" operated by the Federal Bureau of Investigation.

The aptly named system is placed at the Internet service provider level and monitors online communications looking for criminal activity. That may not sound too bad because the FBI claims to actually be looking for criminals, and let's assume for the sake of argument that it is.

There are still two problems with "Carnivore." First, instead of having a warrant to, in effect, tap an Internet user's account for suspected illegal activity, "Carnivore" just taps everyone's communications and like ECHELON, filters them to look for illegal activity. As a result, your private e-mails to your friends and family perhaps discussing very personal family matters, will end up in the hands of the FBI.

This leads to the second problem, namely a clear violation of the Fourth Amendment which is supposed to protect us from such activities performed by the government. Let me remind you of the wording of the Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The FBI's "Carnivore" system completely disregards that amendment because of its broad-sweeping powers to intercept hundreds of thousands of messages at one time from innocent citizens. How does one obtain a warrant to tap hundreds of thousands of e-mail addresses at one time? Moreover, unless a government treats all of its citizens as guilty until proven innocent rather than the reverse, there is no "probable cause" to intercept the enormous amount of e-mail communications, and that too is a violation of the Fourth Amendment.

Since we're talking about cyberspace here, law enforcement is going to have a tough time "describing the place to be searched and the persons or things being seized." Also, since we're talking about cyberspace where evidence is intangible rather than tangible, it would facilitate law enforcement's ability to seize property from one's computer without a warrant.

If you think that would never happen, just look at the recent bill in both houses entitled "The Methamphetamine Anti-Proliferation Act," which gives law enforcement the ability to enter your home or tap your online communications and seize property both on and off-line without your knowledge.

But again, law enforcement has to obtain a warrant to even monitor your online conversations, right? Right, but we have observed over time the ease with which law enforcement obtains warrants to perform wiretaps.

Very few are refused by judges. In fact, it's almost a guarantee

---

Dean is vice president for technology policy at the Free Congress Foundation.

to law enforcement that their requests for warrants will be granted. Since 1968 when Congress passed the wiretap law, 28 requests have been denied out of a total in excess of 20,000. In 1996, one request was denied, the first since 1988. This illustrates a lack of oversight with regard to wiretapping on the part of Congress.

But would a respectable agency such as the FBI really stoop to these sorts of practices? The evidence suggests it has done so already. In addition, in Senate testimony FBI Director Louis Freeh has said, "We need a Fourth Amendment for the Information Age." So, clearly, this agency has little regard for the wording of the one given to us by our Founders because the original amendment would forbid such systems as "Carnivore" and some other questionable surveillance practices conducted by the agency.

Where does the FBI get its authority to conduct these practices? In 1986 Congress passed the "Electronic Communications Privacy Act" to update the federal wiretap law enacted in 1968 by including new communication technologies, such as wireless and electronic communications, under jurisdiction of the existing law.

Then in 1994, Congress, in an attempt to update the law, passed the Communication Assistance for Law Enforcement Act, or CALEA, which essentially told the telecommunications carriers that as its technology developed, it had to design its systems in such a way that it did not impede the ability of law enforcement to conduct wiretap surveillance. CALEA was not to be interpreted as expanding the authority of law enforcement in the area of wiretap surveillance. Very simple.

Immediately after the passage of CALEA, the FBI interpreted the law beyond the boundaries for which it was intended, namely, to include location tracking of cell phone users and "roving wiretaps," allowing law enforcement to obtain a warrant to tap all of the phones within the vicinity of a suspect rather than the traditional practice of tapping a suspect's own telephone line.

The agency also gave itself the authority to design the telecommunications systems throughout the United States. The agency then wanted to further interpret the law to include wiretapping online communications such as e-mail but was refused the authority to do so.

Now comes "Carnivore" which does exactly what the FBI wanted in the first place. Aside from the gross expansion of snooping capability into every computer user's online correspondence, "Carnivore" provides the agency with the ability to carry out procedures which it legally cannot perform, namely the ability to order an ISP to turn over all of the e-mail addresses of users who correspond with a particular suspect or to gain access to the list of an ISP's subscribers.

The boldness and brashness of this federal agency is astounding. While Congress is debating such measures as Social Security or tax reform, issues that it has been haggling over since the Reagan era, it needs to pause and take a sharp look into this agency's practices.

The "Carnivore" system is perfectly named because it is devouring our liberties faster than we can protect them. If we don't start looking into matters such as this which are related to our liberties, congressional debates over education or welfare reform won't make a difference to the future of our nation.

5/24/02 Release - Page 636

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

76 Pages were not considered for release as they are duplicative of DOC #14 OGC FRONT OFFICE FILE (PAGES 45-120)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #29 (Pages 687-762)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

CARNIVORE

(Vol. 67, No. 16)

News

Electronic Surveillance

Existing Laws Permit Collection Of Information From E-Mail, FBI Says

The Federal Bureau of Investigation takes the position that current federal law gives it the authority to implement the use of special software and hardware called "Carnivore" to collect information from the e-mail messages traveling through an Internet service provider's e-mail server, according to testimony by FBI and Justice Department officials July 24 at a congressional hearing. The hearing before the House Judiciary Committee's Subcommittee on the Constitution was convened in response to an uproar triggered by a July 11 article in the *Wall Street Journal* disclosing the existence of Carnivore.

According to the officials' testimony, if an Internet service provider is financially or technologically unable or unwilling to provide information on e-mails pursuant to a court order, the FBI will hook a Carnivore unit up to the ISP's server. Carnivore scans what officials refer to as "the smallest subset" of information from incoming and outgoing e-mail messages. Carnivore then duplicates the information and lets the transmission stream continue to flow.

Carnivore reads the incoming information and filters it according to protocols based on the original court order. Usually, the order will authorize the FBI to collect the "to" and "from" information from messages going to and from a particular e-mail address. Only the relevant information will be recorded. All extraneous information will remain only temporarily in the random access memory and will not be fixed in a stable, recorded format.

The result, according to the FBI, will be a list of e-mail messages that have been sent from or received by a particular e-mail address along with the "to" and "from" information. The FBI likens this to the results obtained by a combination of telephone trap-and-trace and pen register devices, which produce a list of telephone calls to and from a particular number giving only the calling number or the number called.

The FBI has implemented Carnivore 16 times since January and about 25 times overall since it was put into operation two years ago, according to Donald M. Kerr, assistant director of the FBI.

Current Law Authorizes Carnivore. Kevin V. di Gregory, deputy assistant attorney general for the criminal division, testified that the FBI is authorized to implement Carnivore by the current pen register and trap-and-trace law, 18 USC 3121 et seq., and wiretap law, 18 USC 2510-22.

The pen register law allows an FBI investigator to apply for an ex parte order from a court by submitting an affidavit affirming a certification by the applicant that "the information likely to be obtained is relevant to an ongoing criminal investigation." The investigator need not make a showing of probable cause, and the court does not have the discretion to refuse to issue the order.

By following this procedure, the FBI may also obtain from an ISP the "to" and "from" information from incoming and outgoing e-mail messages for a particular address.

Rep. Jerrold Nadler (D-N.Y.) expressed concern that a subject of such scrutiny might never come to know that his privacy had been invaded in such a manner, because the pen register law does not require disclosure if no charges are ever brought.

Di Gregory disputed that any invasion of privacy would have taken place in such a situation. He said that U.S. Supreme Court precedents establishing that a telephone user has no legitimate expectation of privacy in the numbers he dials supports the view that an e-mail user has no such expectation of privacy in the addresses on incoming and outgoing e-mail communications.

According to di Gregory, the FBI may gain access to the content of e-mail messages under the wiretap law. The wiretap law requires a high-ranking officer of the Justice Department to authorize an application for a court order. The court may then issue an order authorizing the government to listen in on a telephone conversation if it finds that there is probable cause to believe that someone is committing, has committed, or is about to commit one of the offenses listed in 18 USC 2516, that there is probable cause to believe that a wiretap will intercept communications concerning that offense, that normal investigative procedures have failed or appear to be unlikely to succeed or are too dangerous, and that there is probable cause to believe that the line to be tapped is the line that is likely to be used for such a communications.

According to Kerr and di Gregory, implementing Carnivore under these statutes will result in minimized and particularized information gathering, and does not amount to a search of all incoming and outgoing e-mail messages traveling through an ISP's server. Additionally, in-house, technological, judicial, and adversarial oversight will ensure that these methods are not abused.

Groups Dispute Claim of Authority. This assertion was flatly contradicted by Barry Steinhardt of the American Civil Liberties Union, who said that such filtering necessarily involves the inspection of every single e-mail message traveling through a server. Such broad authority to filter through private communications was never contemplated by Congress when passing the pen register and wiretap laws, Steinhardt said. Furthermore, he said, no matter what promises the administration makes regarding limiting its data gathering powers, recent history should warn Congress not to believe those promises.

Steinhardt offered as an example the passage of the Communications Assistance to Law Enforcement Act of

Doc. #30

1994, 47 SC 1001 et seq., which resulted from a compromise with law enforcement agencies afraid that new technology would hamper surveillance of telephone calls. He said that in exchange for requiring new digital telephone networks to be constructed to preserve existing surveillance capabilities, the FBI agreed not to use the statute to try to require telephone service providers to create new surveillance capabilities. Nevertheless, according to Steinhardt's testimony, the FBI has "consistently sought greater capacity and new surveillance features that did not exist in 1994. In some cases, they have sought capabilities that they specifically promised the Congress they would not seek."

Filtering out "to" and "from" information is not as easy as the FBI makes it sound, according to Alan Davidson of the Center for Democracy and Technology. Davidson presented the subcommittee with examples of the type of data packets that are collected by Carnivore. In many cases, he said, the "to" and "from" information that the FBI is seeking cannot be obtained without looking in the body of the message.

Both Steinhardt and Davidson, as well as Peter William Sachs, president of New Haven, Conn., ISP ICONN LLC, testified that the type of information that the FBI says it wants from Carnivore can be easily gathered by the ISPs themselves and turned over to law enforcement agencies who have obtained appropriate court orders.

Both Sides Living in the Past. Both law enforcement and civil liberties groups are still thinking in terms of the traditional switched telephone network, according to Stewart Baker, a technology expert with the Washington law firm of Steptoe & Johnson, and former general counsel to the National Security Agency.

Baker said that it is unrealistic to expect ISPs, particularly small ones, to be capable of complying with such an order on its own. "The FBI has got it right," he said. Without Carnivore or some similar program, ISPs would be faced with "an extensive unfunded mandate" to collect information pursuant to court orders.

On the other hand, for the government "to say you don't have an expectation of privacy in information held by a third party is just crazy," Baker said. "Our entire lives are in the hands of third parties."

Some kind of technological solution is necessary for law enforcement to keep up with techno-savvy criminals, he said. At the same time, innocent people must be given protections. Whatever the Congress does decide to do, it must decide quickly, Baker said, or legislation will have been mooted by technological developments.

New Legislation on Horizon. The subcommittee's hearing came a week after a White House official outlined plans by the Clinton administration to introduce a bill that would update both privacy laws and provisions through which wiretapping in all its forms is utilized. The bill, which the White House has yet to send to Congress, would regulate under what circumstances law enforcement could view, listen to and trace e-mails, cellular phone calls, and transmissions over cable networks.

Speaking at the National Press Club July 18, White House Chief of Staff John Podesta said the bill "would amend statutes using outmoded language and that are hardware-specific so that they are technologically neutral. In other words, the legislation would apply equal standards to both hardware and software surveillance."

The White House is characterizing the proposal as one that would increase privacy protections by requiring that court orders authorizing the interception of e-mail be preapproved by high level Justice Department officials. Additionally, the proposal would also make it easier to identify someone who is calling or using electronic means to contact an individual by requiring only one "trap and trace" order to trace a call or Internet session back to the source. Currently, law requires an order to be issued for each separate trace of an e-mail, which are usually bounced around by a number of different Internet services during a transmission, thus requiring multiple orders to trace a single e-mail. Any such orders must be issued by a judge after a factual finding that the standard for criminal activity was met.

The bill also allows for tracing to be conducted without prior court approval in the case of an "emergency," such as actions that threaten national defense, or large-scale hacking attempts. Such orders would be subject to judicial review within a 48-hour period. Another provision would grant authorities the same access to the Internet traffic of consumers using cable modems as those who use dial-up modems.

"With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that customer has watched," Podesta said, "but when cable systems are used to access the Internet through cable modems, we believe the rules should be the tough but sensible standards we also support for e-mails and telephone calls."

Though the White House has no target date for sending up the legislation, the administration is confident they will be able to work with Congress to pass the legislation. "We've been able to strike the middle ground, which will enable us to get there fairly quickly," White House Spokesman Jake Siewert told BNA.

Records

DOJ Agrees to Release of Documents Underlying Report on FBI Crime Laboratory

Over 53,000 pages of background information pertaining to the Justice Department inspector general's investigation of the Federal Bureau of Investigation's crime laboratory are subject to disclosure as a result of the recent settlement of a Freedom of Information Act suit, the National Association of Criminal Defense Lawyers announced July 7. NACDL and its then-press officer, Jack King, were the original plaintiffs in the suit and were later joined by Dr. Frederic Whitehurst, a former employee of the lab whose allegations prompted the investigation.

Besides allowing the plaintiffs to disclose the documents, the settlement calls for the Justice Department to pay $355,000 in attorney's fees and to post a pointer on its website referring inquiries about the documents to NACDL's and Whitehurst's websites.

NACDL spokesman Todd Wells said the organization would make the materials available on compact disc for a cost of $40. Orders can be placed by calling (202) 872-8600.

7-26-00 COPYRIGHT © 2000 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. ISSN 0[illegible]

Content and programming copyright 2000 Cable News Network
Transcribed under license by eMediaMillWorks, Inc. (f/k/a
Federal Document Clearing House, Inc.) Formatting copyright
2000 eMediaMillWorks, Inc. (f/k/a Federal Document Clearing
House, Inc.) All rights reserved. No quotes from the
materials contained herein may be used in any media without
attribution to Cable News Network. This transcript may not
be copied or resold in any media.

CNN

SHOW: CNN TODAY 13:00
July 24, 2000; Monday
Transcript # 00072411V13

TYPE: LIVE REPORT
SECTION: News; Domestic
LENGTH: 301 words
HEADLINE: FBI Defends 'Carnivore' E-Mail Wiretap on Capitol Hill
BYLINE: Kyra Phillips, Pierre Thomas
HIGHLIGHT: FBI officials are on Capitol Hill today defending their new wiretap for the information age. It's called Carnivore and it's designed to selectively monitor computer e-mail to and from a suspect. It can only be used with a court order. Still, critics are concerned about possible privacy violations.

BODY:

THIS IS A RUSH TRANSCRIPT. THIS COPY MAY NOT BE IN ITS FINAL FORM AND MAY BE UPDATED.

KYRA PHILLIPS, CNN ANCHOR: FBI officials are on Capitol Hill today defending their new wiretap for the information age.

It's called Carnivore and it's designed to selectively monitor computer e-mail to and from a suspect. It can only be used with a court order. Still, critics are concerned about possible privacy violations.

More now on the controversy. Here's Justice correspondent Pierre Thomas.

Hi, Pierre.

PIERRE THOMAS, CNN JUSTICE CORRESPONDENT: Hi, Kyra. As you pointed out, the FBI says Carnivore is a new investigative tool which can tap into the e-mail of a suspect, but only with a court order. But critics say it's Big Brother on the Internet. And today, Congress wanted answers.

(BEGIN VIDEO CLIP)

UNIDENTIFIED MALE: Even a system designed with the best of intentions to legally carry out essential law enforcement functions may be a cause for concern if it's use is not properly monitored.

REP. JOHN CONYERS (D), MICHIGAN: Constitutional rights don't end where cyberspace begins.

(END VIDEO CLIP)

THOMAS: But the FBI was quick to point out the restrictions that govern Carnivore. The FBI's top lab official explained the safeguards.

(BEGIN VIDEO CLIP)

UNIDENTIFIED MALE: In every case we require a court order. That court order is specific to the numbers we target, if you will, the addresses we can target.

Doc 31

(END VIDEO CLIP)

THOMAS: Today was a fact-finding hearing and there was one point of early agreement: Carnivore may not be the best name for this system -- Kyra.

PHILLIPS: All right, Pierre Thomas, thanks so much.

TO ORDER A VIDEO OF THIS TRANSCRIPT, PLEASE CALL 800-CNN-NEWS OR USE OUR SECURE ONLINE ORDER FORM LOCATED AT www.fdch.com

LANGUAGE: ENGLISH

LOAD-DATE: July 24, 2000

Copyright 2000 Phillips Business Information, Inc.
COMMUNICATIONS TODAY

July 24, 2000

SECTION: Vol. 6, No. 140
LENGTH: 1097 words
HEADLINE: From the Editor's Desk... Paul Coe Clark III
BODY:
Who's Afraid Of The Big, Bad Carnivore?

This week, it finally happened: the government made clear its intent to expand wiretapping from switched voice traffic to Internet traffic. The implications for Internet-service providers and cable operators are enormous.

Last Monday, White House Chief of Staff John Podesta proposed a bill to (in my assessment) expand the voice wiretapping allowed under the Communications Assistance for Law Enforcement Act to e-mail. Podesta defended the FBI's "Carnivore" packet-sniffing software, which allows the government to read the address information and content of e-mail.

My coverage of the proposal (CT 7/18) was quite restrained, as I wanted to give it fair scrutiny before judging it.

I've given the plan that scrutiny, and I think it's a bad one. Here are two reasons why:

1) The administration avoided honest debate on the rationale for spying on citizens. Podesta, in particular, misrepresented the uses of wiretaps. He also was misleading in saying there had been no improper voice wiretaps, a "fact" he used to support IP wiretapping.

FBI and Justice Department officials, in testimony to Congress, inevitably tout wiretapping as a solution to terrorism and child pornography -- political hot-button crimes everyone opposes. That testimony draws favorable press coverage and congressional support. Who wants to be portrayed as supporting those crimes?

Podesta hit the same theme in describing Title III of the 1968 Crime Control and Safe Streets Act, which set the rules for voice wiretapping. The administration wants to apply Title III-type rules to Internet spying.

"It only allowed wiretaps in the most serious crimes, such as espionage, treason and crimes of violence," Podesta said.

But those are rarely the crimes against which law enforcement uses wiretaps. The 1999 wiretapping report by the Administrative Office of the United States Courts (available on the Web site of the Electronic Privacy Information Center) shows there were 1,350 Title III wiretaps last year. There were only 174 in 1968.

The report includes a breakdown of the crimes that were the basis for each wiretap. A full 978 of the wiretaps in 1999 were drug cases. Agencies rarely mention that fact when seek wiretapping authority, because they know it weakens their argument. Tap our phones because terrorists might blow someone up? Maybe so. Tap them because someone, somewhere, is smoking a joint? I don't know.

Drug cases were followed by racketeering (139 cases). Only when we get to homicides/assaults (62 cases) do we hit the "crimes of violence" cited by Podesta. National-security wiretaps do not even come under Title III, but the Foreign Intelligence Surveillance Act. There were 886 wiretaps under FISA in 1999. No breakdown of those cases is available, so we can't tell if they were indeed for treason and espionage. The FBI, of course, has a history of using national-security authority to wiretap such notorious menaces to the common weal as Martin Luther King Jr., John Lennon, and any reporters who happen to annoy Richard Nixon.

DOC #32

Podesta said that all wiretapping has met Title III standards. "I know of no case in which a wiretap was thrown out" for violating those standards, he said. Not yet, maybe. But the current Ramparts police scandal in Los Angeles resulted in testimony about hundreds, if not thousands, of illegal wiretaps. I asked Podesta how he could reconcile that fact with his statement. Neither he nor his aides could. They had no answer.

2) Carnivore IP wiretapping is fundamentally different from CALEA voice wiretapping. Taps on switched phone circuits, by their nature, record only the phone calls and tracing information of individual lines. Carnivore, by its nature, must intercept all traffic through an ISP to find the suspect messages. We have nothing but the government's assurances that it will ignore traffic for which it has no warrant.

Carnivore also can read content of e-mails, as well as addressing information. Under Podesta's proposal, the government standard for intercepting address information would be lower, as it is for pen-register and track-and-trace information for voice calls. A pen-register intercept, however, does not give access to the voice call. Carnivore gives access to the text of e-mails. Again, we have only the government's assurances that it will ignore the content.

Not all elements of the Podesta proposal are bad. He proposes requiring probable cause (the Title III standard) to intercept the content of e-mail. And one element, the removal of the protections against cable surveillance in the Cable Act of 1993, is inevitable. Whatever rules result from this legislation should surely apply evenly to ISPs of all technological stripes.

The depressing thing is how eagerly the phone industry now supports CALEA. The Telecom Industry Association was involved in developing the J-STD-025 wiretapping standard and Carnivore, which was unveiled late last month at the TIA-organized Joint Experts Meeting in Washington. "The FBI's program is extremely sophisticated," TIA said Tuesday. Carnivore works with Microsoft Outlook, Lotus Notes and other e-mail programs, the association continued.

Equipment vendors, who originally balked at CALEA, now consider wiretapping a profit center. ADC [ADC] just rolled out its NewNet CALEAserver wiretapping line. "It receives the intercepted communications data from various circuit-switched network elements, processes it to conform to the requirements of J-STD-025, and then distributes it to the appropriate LEA collection facilities," the company said proudly Thursday.

Comverse Infosys [CMVT] also rolled out gear this week. "Comverse Infosys is the industry leader in the legal interception market worldwide," President Dan Bodner bragged.

Current rumblings suggest ISPs are less happy about spying on their customers. Don't be fooled, though -- they'll do it. The Podesta proposal and CALEA should be stopped before spy equipment becomes an inextricable part of our basic communications network.

Paul Coe Clark III is the editor of Communications Today. He can be reached at (301) 340-7788, ext. 2037, or at pclarkfphillips.com.

LANGUAGE: ENGLISH

LOAD-DATE: July 24, 2000

Copyright 2000 CNBC, Inc.
CNBC News Transcripts

SHOW: RIVERA LIVE (9:00 PM ET)

July 24, 2000, Monday

LENGTH: 1375 words
HEADLINE: WHETHER THE GOVERNMENT SHOULD BE ALLOWED TO INTERCEPT INTERNET E-MAILS
ANCHORS: DAN ABRAMS
REPORTERS: JOE JOHNS
BODY:

Mr. DONALD KERR (Director, Lab Division, FBI): Hackers break into financial service company systems and steal customers' home addresses and credit card numbers. Criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques to--designed to work with new and evolving computer and network technologies.

DAN ABRAMS, host:

But how far should law enforcement be permitted to go to combat criminals? Should they be able to tap into someone's e-mail to see what is sent out and received? The FBI says yes, and they say they now have a new surveillance system that can isolate a suspect's messages without invading the privacy of others, an electronic strainer of sorts. They say it has the same effect as a phone wiretap, a rarely used technique to monitor a specific suspect with permission from a judge. But others say the FBI's new Carnivore system, as it is known, is an invasion of privacy, that it's nearly impossible to isolate only the relevant e-mails and that the FBI would have access to far too much information. Today the debate landed on Capitol Hill. NBC's Joe Johns reports.

JOE JOHNS reporting:

Fears that e-mail from law-abidding users of the Internet could be swept up in a new FBI computer system designed to catch terrorists, con artists and hackers led Congress to schedule today's hearing. But some on Capitol Hill say drastic action may be needed to put the brakes on the FBI e-mail, wiretap system known as Carnivore.

Representative RICHARD ARMEY (Republican, Majority Leader): Well, I would shut down Carnivore now if I were at the agency.

JOHNS: Carnivore is a computer application installed on a PC that agents connect to the hardware of an Internet service provider to search for specific senders and receivers of messages. The FBI needs a court order to use it and says only targeted information is retrieved, that no indiscriminate snooping is allowed.

Mr. KERR: We're not in the, you know, broad surveillance business in any way. We're a law enforcement agency limited in what we do by what the courts order us to carry out.

JOHNS: But many Internet service providers don't like it.

Mr. CHARLES ARDAI (Juno Online Services): I think our customers would not take kindly to the idea that their private information could be available to a government agency.

JOHNS: Still one scholar who specializes in privacy issues says it's a tool law enforcement needs.

Doc. #33

Mr. AMITAI ETZIONI (George Washington University): Now more and more communications advance through the Internet. And without intercepts, we--the FBI cannot do its job.

JOHNS: Even if Congress is persuaded that Carnivore does not invade privacy, the system may still face a challenge. The American Civil Liberties Union has filed a Freedom of Information request demanding Carnivore computer codes that the government wants to keep secret. Joe Johns, NBC News, the Capitol.

ABRAMS: Joining us now from Washington is Ari Schwartz from the Center for Democracy and Technology. He's an expert on privacy and the Internet. Nancy Grace and Michael Nasatir remain with us to discuss Carnivore and cybersnooping by the feds.

Mr. Schwartz, let--let me start with you. Why is this any different, in effect, than a wiretap?

Mr. ARI SCHWARTZ (Analyst, Center for Democracy and Technology): Well, it's different in a few ways. The--the biggest difference right now is that with--with a digital wiretap, we know we have the technology--we know what is--what--what the tap--what kind of taping is going on. This system is completely closed. It's a black box that's put on to the Internet service provider. Even the Internet service provider doesn't know how it works. That's much different than the way that phone--than--than phone wiretapping happens now.

ABRAMS: Yeah. But the FBI's given these demonstrations to various people to say, 'Look, we've got a method in place. We've got a system which is going to, in effect, treat this like a phone tap. We can isolate exactly which person's e-mails we want to tap into.' And with, you know, all of the cyberterrorism, in addition to the non-cyberterrorism which is occurring through the Internet, I think a lot of people are saying, 'I'd feel a lot more comfortable if I know that my FBI can be snooping on possible terrorists.'

Mr. SCHWARTZ: Well, the--there's n--there's nothing at--we--what we need is balance, and that's really what we're getting at here, is we need a balance between privacy and--and the--the kind of searches that you're talking about. The problem that we've seen is that--the difference of showing a demo about what--what gets pulled out is different than s--than knowing the technology, knowing what's kept in the logs, what can be retrieved later on. That's much different. As I said, we have the code for--for the phone tapping system. Why can't we just see the code in this case?

ABRAMS: And--and--and what is the argu--the argument on the other side is that it's patent protected and that it would allow hackers to break into it, right?

Mr. SCHWARTZ: Well, th--that's what their--that's what their concerns are. But, of course, again, as I said, we have the same--we have the same thing set up with the digital phone network. We've had hackers in the--in the phone networks as well. You know, why can't we--we should just be able to see this code and have it open.

ABRAMS: And--and so that's your--that's your primary grip. I mean, is your--if--if...

Mr. SCHWARTZ: Well, that--that--that's the main concern with Carnivore right now. The other concern that Carnivore raises and shows for the future is the question of the decay of the Fourth Amendment. We're having a lot more information now stored on computer systems and on third-party systems than we ever have in the past. When the framers of the Constitution wrote the Fourth Amendment, which is protections from unreasonable searches and seizures by the government, people had the files in their home. The government had to come and knock on their door. That's not the case today.

ABRAMS: Nancy Grace, Fourth Amendment problem?

Ms. NANCY GRACE (Anchor, Court TV): Well, you know, of course that's not what the framers had in mine when they wrote the Constitution. But, Dan, the Fourth Amendment has been applied for everything from abortion rights to what you carry in your car trunk. It can certainly be applied to computer access. My only concern is, you know, years and years and years of Fourth Amendment law regarding wiretap has developed over the past decades, and that same law needs to be applied now to intercepting Internet communications. It cannot be a fishing spree on the part of the government. On the other hand, a warrant allows you to open doors, open boxes, open mail and open the Internet.

ABRAMS: Got to take a break. Our topic this part is Big Brother's Watching. When we come back, we're going to talk about a sheriff who is putting Web cams in his prison. We'll be back in a minute.

(Announcements)

ABRAMS: Before we get to the sheriff who has installed Web cams in his prison, I want to talk to Michael Nasatir about this issue of this FBI program that you can attach to Internet service providers to basically look at what people are e-mailing. What do you think?

Mr. MICHAEL NASATIR (Criminal Defense Attorney): You know, I think what the gentleman from Washington is saying is, 'Look, let's--let's let the civil libertarians have a crack and see what they're really going to do. It cannot be a secret. The technology has got to be--we've got to be able to study it to know what we're objecting to or not objecting to. And at the very least I do agree with Nancy Grace. Let them get a court order for--and keep it specific and have the F--Fourth Amendment apply for sure.

ABRAMS: Well--and I think there's no question that there would be--they'd have to make an application for a warrant the same way they do with a wiretap. I want to thank Ari Schwartz for joining us and talking about this topic.

LANGUAGE: English

LOAD-DATE: July 25, 2000

Copyright 2000 Burrelle's Information Services
ABC NEWS

SHOW: WORLD NEWS THIS MORNING (6:00 AM ET)

July 24, 2000, Monday

TYPE: Newscast
LENGTH: 324 words
HEADLINE: FBI E-MAIL SURVEILLANCE PROGRAM COMES UNDER FIRE
ANCHORS: ANDERSON COOPER
REPORTERS: ANDREA McCARREN
BODY:

ANDERSON COOPER, anchor:

Federal agents say they've come up with a high-tech way to find criminals who use cyberspace to plan illegal acts, but critics contend the system, called Carnivore, simply goes too far. That is the focus of a hearing on Capitol Hill today. Here now is ABC's Andrea McCarren.

ANDREA McCARREN reporting:

(VO) The FBI says Carnivore is an essential law enforcement tool to police in the rapidly growing world of cyberspace.

Mr. DONALD KEER (Assistant Director, FBI): The range of crimes that are facilitated by computers didn't exist before, so we now have Internet fraud rather than fraud on paper.

McCARREN: (VO) The technology allows the FBI, with a court order, to sift through thousands of private e-mails selecting out those to and from a particular criminal suspect, but privacy advocates say the system is too broad because it sorts through the private e-mail of innocent people, too.

Mr. AL GIDARI (Privacy Specialist): It's a little bit like looking at all the cars on a highway just to find the blue Honda you want, and it's--it's extremely intrusive.

McCARREN: (VO) The Clinton administration proposed that the strict privacy standards that apply to telephone service be extended to electronic communications.

Mr. JOHN PODESTA (White House Chief of Staff): What we're interested in is coming up with a balance that accounts for the needs of law enforcement to pursue--pursue organized crime and narcotics traffickers but also protects the privacy of individual Americans.

McCARREN: (VO) Over the last year, the FBI has used Carnivore in about 25 criminal investigations.

(OC) Now, amid growing privacy concerns, the agency plans to submit Carnivore to a third party for an independent assessment. The FBI wants to keep secret how the technology works but, at the same time, reassure the public that their online privacy is protected. Andrea McCarren, ABC News, Washington.

LANGUAGE: English

LOAD-DATE: July 25, 2000

Doc #34

Copyright 2000 Burrelle's Information Services
ABC NEWS
SHOW: WORLD NEWS TONIGHT (6:30 PM ET)

July 24, 2000, Monday

TYPE: Newscast
LENGTH: 442 words
HEADLINE: PRESIDENT CLINTON RETURNS TO CAMP DAVID TO ASSIST IN PEACE TALKS; BI DEFENDS E-MAIL MONITORING SYSTEM
ANCHORS: PETER JENNINGS
REPORTERS: JOHN COCHRAN
BODY:

PETER JENNINGS, anchor:

At Camp David in Maryland, day 14. The Israeli and Palestinian leaders have been holed up for two weeks now with hardly a leak to the news media, which in itself is quite remarkable. President Clinton, just back from Japan, spent much of last night and most of today in the talks, desperately, we are told, trying to coax the parties into some kind of a deal. ABC's John Cochran is covering Camp David for us.

John, looking at your notes today, 'Not looking good, senior administration officials will take a miracle,' say the Palestinians, doesn't look good at all?

JOHN COCHRAN reporting:

That's right, Peter. A senior administration official told me, just a short time ago he believes the talks will end one way or the other this week and he was not particularly optimistic. On top of that, Palestinian officials told ABC News, they believe it will take a miracle to achieve a breakthrough. The key stumbling block, not the only stumbling block, but the key one, continuing to be Jerusalem. So much so, that today, the negotiators simply took that subject off the table and concentrated on other issues.

JENNINGS: So why did they take--John, John, why do they take Jerusalem off the table and expect they can get anywhere like a deal?

COCHRAN: Well, what they would like to do is to try to get an agreement on land and security and they are getting the director of the CIA, George Tenet, to help them on this security issue. If they can resolve those issues, maybe they can go back to--to the issue of Jerusalem. What they would like, Peter, is to get at least a partial agreement this week, something that will enable both sides to come back at least in August and keep banging away.

JENNINGS: OK, John Cochran covering Camp Maryland for us. There's the key phrase, partial deal. Jerusalem has always, always been the final issue.

The FBI was on Capitol Hill today defending its e-mail monitoring system, the ominous-sounding Carnivore, against concerns that it casts too wide a net. The agency told Congress today it only uses the system to eavesdrop on suspected terrorists, computer hackers and other criminals, not on law-abiding citizens. Some people will not be convinced.

When we come back, a plague of grasshoppers in Texas.

Mr. JAMES ROBINSON (Entomologist): These are some of the worst outbreaks of insects for our cattlemen in the state that I've witnessed.

JENNINGS: And surviving a storm off the Louisiana coast. Was it murder or self-preservation?

DOC. #35

Announcer: WORLD NEWS TONIGHT with Peter Jennings and A CLOSER LOOK, brought to you by...

(Commercial break)

LANGUAGE: English

LOAD-DATE: July 25, 2000

Copyright 2000 Burrelle's Information Services
CBS News Transcripts

SHOW: CBS EVENING NEWS (6:30 PM ET)
July 24, 2000, Monday

TYPE: Newscast
LENGTH: 462 words
HEADLINE: NEW SURVEILLANCE SOFTWARE ALLOWS THE FBI TO SNOOP THROUGH COMPUTER USERS' E-MAILS
ANCHORS: JOHN ROBERTS
REPORTERS: JIM STEWART
BODY:

JOHN ROBERTS, anchor:

Top officials of the FBI went to Capitol Hill today to respond to lawmakers' concerns about a sophisticated e-mail surveillance program and its potential for abuse. Critics fear this new software makes government snooping so easy, it leaves ordinary Americans vulnerable to invasion of privacy. CBS' Jim Stewart has more.

JIM STEWART reporting:

Every day, more than a billion e-mails are sent and received by computer users, and the FBI thinks criminals are now just as fond of them as the next guy. But the problem for agents has always been: Just how do you sort through all the gibberish to find any meaningful evidence? Today, the bureau told Congress it thinks it's found the answer in a software program called Carnivore.

Mr. LARRY PARKINSON (General Counsel, FBI): This is--despite its unfortunate name, this is a tool that is very surgical.

STEWART: Essentially, Carnivore is like a wiretap on the Web. Physically, it's nothing more than a small computer the FBI can lock inside the switching room of an Internet service provider like, say, America Online. But instead of reading every AOL customer's e-mail, it's designed to zero in and record just the messages sent to and from one particular e-mail address.

Mr. DONALD KERR (Director, Lab Division, FBI): We don't do broad searches or surveillance with this system. That's not authorized by a court order and, in my view, could not be.

STEWART: Critics, however, immediately asked: Who's watching the watchers?

Mr. ALAN DAVIDSON (Center for Democracy & Technology): Carnivore has access to much more information than it is legally entitled to collect. How do we know that we can trust Carnivore? How do we know what kind of leash has been put on Carnivore?

STEWART: The reason for the skepticism is because there's a big difference between wiretapping the Internet and wiretapping a telephone. If the FBI wants to bug your telephone, they get a court order and go to the phone company, and the phone company makes the connection for the bureau. If the FBI wants to wiretap your Internet address, they get a court order and then they can make the connection themselves.

They've done it 16 times this year already, mostly against Internet hackers, and the potential list of suspects and their crimes is growing, agents warned. Four years from now, the number of commercial e-mail messages alone is expected to top 200 billion a year. Jim Stewart, CBS News, Washington.

ROBERTS: And next up on the CBS EVENING NEWS, a new scheme to bilk the old

and steal their trust.

(Graphic on screen)

CBS MarketWatch

DOW JONES INDUSTRIALS

CLOSE down 48.44 10,685.12

NASDAQ

CLOSE down 112.88 3,981.57

CBS.MARKETWATCH.COM

(Announcements)

LANGUAGE: English

LOAD-DATE: July 25, 2000

Copyright 2000 Burrelle's Information Services
CBS News Transcripts

SHOW: THE OSGOOD FILE (Various Times)

July 25, 2000, Tuesday

TYPE: Commentary
LENGTH: 445 words
HEADLINE: FBI UNDER FIRE FOR USING INTERNET SOFTWARE TO WATCH SUSPECTS' E-MAILS
REPORTERS: CHARLES OSGOOD
BODY:
CHARLES OSGOOD reporting:

THE OSGOOD FILE. Charles Osgood on the CBS Radio Network.

The FBI is able to read supposedly private e-mail and other Internet traffic using a system called Carnivore. Carnivore, according to the dictionary, is any flesh-eating animal or plant. Not to worry, says the FBI.

Mr. LARRY PARKINSON (General Counsel, FBI): Despite its unfortunate name, this is a tool that is very surgical.

OSGOOD: Where have we heard that before? Stand by.

(Announcements)

OSGOOD: The American Civil Liberties Union is concerned, to say the least, about the FBI's Carnivore system for snooping on the Internet.

Unidentified Man #1: This is the equivalent of going to the post office and stationing an FBI agent there looking at the addressing information of every letter that goes through.

OSGOOD: No, it's nothing like that at all, says the FBI Lab Division's Donald Kerr.

Mr. DONALD KERR (FBI Lab Division): We don't do broad searches or surveillance with this system.

OSGOOD: 'The bureau is being very scrupulous about not violating anybody's civil rights with Carnivore,' says the FBI general counsel Larry Parkinson.

Mr. PARKINSON: This is a tool that is deployed rarely and it is never deployed without a court order.

OSGOOD: In other words, 'Trust us.' 'Not good enough,' says Alan Davidson of the Center for Democracy and Technology.

Mr. ALAN DAVIDSON (Center for Democracy and Technology): Carnivore has access to much more information than it is legally entitled to collect. How do we know that we can trust Carnivore? How do we know what kind of leash has been put on Carnivore?

OSGOOD: The Justice Department says law enforcement officials have to follow crime wherever it leads. Deputy attorney general Kevin DiGregory.

Mr. KEVIN DiGREGORY (Deputy Attorney General): Many of the crimes that we confront every day in the physical world are beginning to appear in the online world.

OSGOOD: For many of the abuses that occur in the physical world occur in the online world, too. That's why Congress is now taking an interest in

DOC. #37

Carnivore. John Conyers, Democrat of Michigan.

Representative JOHN CONYERS (Democrat, Michigan): Constitutional rights don't end where cyberspace begins.

OSGOOD: And if the FBI is as scrupulous about using Carnivore as it says it is, there's always Murphy's Law to consider. That's the one that says, 'If anything bad can happen, it will.' Republican Congressman Spencer Bachus of Alabama.

Representative SPENCER BACHUS (Republican, Alabama): The potential for abuse here's tremendous.

OSGOOD: THE OSGOOD FILE. Charles Osgood on the CBS Radio Network.

LANGUAGE: English

LOAD-DATE: July 25, 2000

Copyright 2000 U.P.I.
United Press International

July 25, 2000, Tuesday

SECTION: GENERAL NEWS
LENGTH: 956 words
HEADLINE: On The Net
BYLINE: By United Press International
BODY:

Justice Department officials defended its "Carnivore" e-mail scanning program on Monday in front of a House panel, saying it is "narrowly focused" and they have used it just 25 times in two years, including 16 times so far this year. "Discriminating between users' messages on the Internet ... is exactly what Carnivore does," said Donald Kerr, assistant director at the FBI. "It does not search through the contents of every message and collect those that contain certain key words like 'bomb' or 'drugs.' It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user." Kerr told the House Judiciary Subcommittee on the Constitution that all but six uses of the program this year have been for "national security reasons," but he declined to talk about the cases. Attorney General Janet Reno has ordered an independent review of the system to determine whether it infringes on privacy rights. The American Civil Liberties Union has filed a Freedom of Information Act request with the department for all documents related to Carnivore. 0-

Another Internet file-trading service is facing a lawsuit by Hollywood heavy-hitters. Scour.com, a site that searches the Internet for music and video files and allows users to exchange them, is the target of a copyright infringement suit filed in New York by the Recording Industry Association of America and the Motion Picture Association of America. Scour.com, which is backed in part by former Disney head Michael Ovitz, said it was "very surprised" by the lawsuit, because the company had been in recent talks with top industry players such as Sony. MPAA Chairman Jack Valenti called the site "Napster with movies." 0-

The recording industry's case against Napster, meanwhile, goes to trial on Wednesday in San Francisco. Lawyers for the major record labels are expected to ask a judge to shut Napster down because it allegedly promotes music piracy and copyright infringement. Napster allows users to share MP3 digital recordings of songs that are compact-disc quality and can be downloaded in a few minutes. "The fact is that Napster has given millions and millions of music fans the opportunity to hear music they haven't heard before," said Napster CEO Hank Barry to the New York Times. Experts watching the case don't expect it to end quickly-the issues are complicated, and Napster has amassed a battled-hardened legal team on its side. 0-

Napster's case has recently drawn a lot of the media's attention, but the high-tech world's biggest case is still simmering in the background. A federal judge found in June that Microsoft had used illegal and unfair tactics to push its Windows operating system, and the company has one appeal left - to the Supreme Court. But the case might have one last detour. Microsoft wants to apply a federal antitrust law enacted in the 1970s that would allow a lesser court to hear the appeal first. According to the Washington Post, the company's lawyers believe the Supreme Court would benefit from another review of factual and procedural issues in the case. The government and the company can file more paperwork on the issue in August, and the Supreme Court could make a decision by the fall on whether it will hear the appeal. 0-

Stephen King said he offered his new serial novel "The Plant" on the Web for a "buck an episode" because he wanted to test how people would respond. "We have a generation of computer jockeys that we've raised on Napster and MP3

Doc. #38

who have gotten ... the mistaken idea that everything in the store is free. And I'd like to see if we can't reeducate these people to the idea that the fruits of talent cost you money," the author said Monday on ABC's "Good Morning America." Readers can download the first two portions of the book without paying the $1, but according to King on his Web site, "If you don't, the story folds." He wants 75 percent of all readers to pay for the story in order to keep it going. It's available at: http://www.stephenking.com/download.html 0-

A French judge has ordered a series of tests into whether Internet screening software works well enough to require Yahoo! to block French Web surfers from having access to online auctions of Nazi memorabilia. French law prohibits the sale or exhibition of items with racist overtones, so a judge in June ordered the Web company to block access to the auctions. Because such auctions are legal elsewhere, Yahoo! only cut them from its France-oriented fr.yahoo.com site, not its main, global Yahoo.com portal. The company argued that it doesn't have the means to keep French users from accessing all the auctions outside of fr.yahoo.com, but Judge Jean-Jacques Gomez said that idea should be tested by experts before he makes another ruling in August. Yahoo! could face hundreds of thousands of dollars in fines. 0-

Rivals of America Online's instant messaging service have banded together in an attempt to get the Virginia company to open up its huge community of real-time Internet chatters. The MSN Network, AT&T Corp., iCast Corp. and Tribal Voice have formed a coalition called IMUnified that will push AOL to let them connect to its IM service, which has tens of millions of users. The group might end up with the government on its side - the IM issue is one of many that the Federal Communications Commission will consider on Thursday when it holds a hearing on the proposed AOL-Time Warner merger. IMUnified has an uphill battle ahead according to industry analysts. Mark Levit of International Data Corp. told Computerworld that AOL will only give in when it is certain its IM market share won't be affected. 0-

LANGUAGE: ENGLISH

LOAD-DATE: July 26, 2000

Copyright 2000 National Public Radio (R). All rights reserved. No quotes from the materials contained herein may be used in any media without attribution to National Public Radio. This transcript may not be reproduced in whole or in part without prior written permission. For further information, please contact
NPR's Permissions Coordinator at (202) 414-2000.
National Public Radio (NPR)

SHOW: MORNING EDITION (11:00 AM on ET)
July 25, 2000, Tuesday

LENGTH: 584 words
HEADLINE: FBI'S SYSTEM TO MONITOR E-MAILS GOING THROUGH INTERNET SERVICE PROVIDERS CALLED UNCONSTITUTIONAL BY MANY
ANCHORS: BOB EDWARDS
REPORTERS: LARRY ABRAMSON
BODY:

BOB EDWARDS, host:

The FBI is struggling to defend a controversial wiretapping system for the Internet. The system is called Carnivore. It's designed to help investigators search for evidence by sifting through huge volumes of e-mail. Civil liberties groups say Carnivore exposes law-abiding citizens to an FBI investigation. The FBI told members of Congress yesterday that the system can be trusted because it only examines messages relevant to investigations. NPR's Larry Abramson reports.

LARRY ABRAMSON reporting:

Usually the FBI asks Internet service providers to do its eavesdropping work, but if an ISP cannot supply the right information, the agency has been turning to Carnivore. Despite its ominous name, Carnivore is just a computer with special software. The FBI installs the system in the offices of the Internet service provider. Like a big vacuum cleaner, Carnivore sucks up every single e-mail message sent or received through the provider. But according to the FBI's Donald Kerr, Carnivore spits out everything except for the few bits that are related to the investigation.

Mr. DONALD KERR (FBI): What it's basically allowing us to do is record the address to which the envelope is being sent and the return address on the outside of the envelope. We're not permitted to read the subject line and, in fact, do not capture that and record it.

ABRAMSON: It's a lot harder for the FBI to get court authority to actually open up e-mail messages. The FBI assured members of a House Judiciary subcommittee that Carnivore software can be carefully tailored so that it only traps the names of the sender and the recipient of a message. Agents have used these kinds of searches on telephone lines for decades. Kevin Di Gregory, with the Department of Justice, says they're very useful in the early stages of an investigation.

Mr. KEVIN Di GREGORY (Department of Justice): To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products or to whom the drug dealer is selling his goods. It is, therefore, important to determine with whom the drug dealer is communicating.

ABRAMSON: The problem is that the system has to peek at each bit of information so that it can decide what to throw away. Many members of the Congress and civil liberties groups are not ready to trust the FBI when it says it really will discard information it's not allowed to collect. Barry Steinhardt of the American Civil Liberties Union called the potential for abuse unprecedented.

Mr. BARRY STEINHARDT (American Civil Liberties Union): Never before has law

DOC. #39

enforcement installed a device which access all the communications of a service providers customers rather than only the communications of the target of a particular order.

ABRAMSON: Internet service providers have become accustomed to court orders and subpoenas for information in criminal investigations and lawsuits. But many say they resent the FBI's use of Carnivore. They say the system poses a security threat and can crash an ISP's computers. Congressman Bob Barr of Georgia accused the agency of abusing its authority and bullying its way on to the premises of Internet service providers.

Representative BOB BARR (Georgia): You're saying, 'What we're going to do is we're going to go outside of the law here basically and we're going to force you to allow us to put our software into your system. You will not be able to monitor it. It's completely unsupervised. Thank you very much, guys. You just give us access and we'll do our thing.'

ABRAMSON: Much of the Carnivore debate hinges on just what Internet users expect when they send e-mail. Courts have ruled that telephone callers have no right to expect that the telephone numbers they dial will be kept private. But Stuart Baker, former general counsel at the National Security Agency, says extending that analogy to Internet service providers doesn't make sense.

Mr. STUART BAKER: To say you don't have an expectation of privacy in information that is in the hands of the third party in the Internet age is just crazy. I mean, our entire lives are in the hands of third parties.

ABRAMSON: The FBI is offering to hire an independent investigator to prove that Carnivore offers a constitutional way to wiretap on the Internet. But so far, the agency says it will not reveal the software code behind the system. Many civil libertarians say that's the only way they can prove to Congress that Carnivore is dangerous and should be abandoned. Larry Abramson, NPR News, Washington.

LANGUAGE: English

LOAD-DATE: August 7, 2000

Copyright 2000 Chicago Tribune Company
Chicago Tribune

July 25, 2000 Tuesday, CHICAGO SPORTS FINAL EDITION

SECTION: News; Pg. 1; ZONE: N
LENGTH: 989 words
HEADLINE: FBI DEFENDS USE OF E-MAIL MONITORING SOFTWARE
BYLINE: By Frank James, Washington Bureau.
DATELINE: WASHINGTON
BODY:

Privacy experts and lawmakers on Monday criticized the FBI for using technology that monitors e-mail, claiming that it threatens privacy rights. But computer security experts say those concerns miss the point: By its very nature, e-mail is not secure. Electronic messages are among the worst ways to send private information.

Speaking after a House Judiciary subcommittee hearing Monday, Tom Perrine, a computer expert, lamented that he ran out of time before he could explain to lawmakers that it's not just government snoops using a special, secret software program like "Carnivore" that threaten e-mail privacy.

Anyone with a little computer know-how can catch and read other people's online mail. The answer, he and other experts say, is a simple encryption program that codes the e-mail so others can't read it.

"If everyone used strong encryption, large parts of Carnivore would be completely useless," Perrine said.

At the 3 1/2-hour hearing, Democratic and Republican skeptics openly doubted the FBI's ability to keep from abusing its Carnivore technology and violating Americans' constitutional rights with the Internet equivalent of a telephone wiretap.

For two years, witnesses testified, the agency has quietly used Carnivore to capture the "to" and "from" lines of e-mail between certain suspects and their e-mail buddies. When federal judges have provided the agency with the required authority, the FBI also has captured not just the address information, but the content of targeted e-mails.

Privacy experts, lawmakers and others have sharply criticized the FBI for its use of the program; Monday's hearing was filled with accusations of privacy violations.

"I think Congress has to act," said Rep. Jerrold Nadler (D-N.Y.), calling for tighter restrictions on the FBI. "Police agencies can't be afforded untrammeled discretion, and we can't assume a lack of bad intent on the part of police or the presence of goodwill is enough to protect people's privacy."

The FBI's general counsel, Larry Parkinson, assured the lawmakers: "There are checks and balances with respect to Carnivore. ... It's not a situation where a rogue FBI agent could broaden the coverage of the Carnivore intercept and violate the court order" authorizing the surveillance.

What the numerous witnesses defending the use of Carnivore, as well as privacy advocates condemning it, didn't acknowledge, however, was the thing they all agree on--the insecurity of e-mail in general.

President Clinton knows. After a speech last March in Silicon Valley, as reported by Dan Gillmor, technology columnist for the San Jose Mercury News, someone asked Clinton if he keeps in touch with his college student daughter, Chelsea, by e-mail while she is away at Stanford University.

Doc. #40

"I don't do e-mail with Chelsea. Absolutely not--I don't think it's secure," said Clinton.

Indeed, said Perrine, manager of security technologies at the San Diego Supercomputer Center, at the University of California-San Diego, everyone worries about protecting their computers, but too many send sensitive information by e-mail.

"There's a quote, I wish I could remember who said it, but basically it goes ... 'Trying to do secure things over the Internet is like two people in concrete bunkers surrounded by machine guns sending messages to each other written on the back of postcards,'" Perrine said.

"There's all this communication that goes across that can be read by anyone" with access to the network and technology called a packet sniffer, he said.

E-mail transmitted over the Internet, like all information sent over the global network, is broken into chunks called packets that are bounced from the sender's computer to the recipient's. Because of the way the Internet was constructed, the packets often take different routes to get from point A to point B, bouncing around the Internet until they arrive at their destination and are reassembled.

At the right place on the network, a hacker or someone else using a packet sniffer can collect the packets then reassemble them to learn the contents of an e-mail, leading to the security issue Clinton raised.

The greatest cause for concern is the possibility of an inside job, someone with access to the powerful computers known as servers, the brains of computer networks, said Richard Smith, an Internet security expert based in Cambridge, Mass.

"In the case of Chelsea, the concern I would have as President Clinton or the Secret Service is that somebody at Stanford, or wherever, who maintains the e-mail system was watching that traffic, that they got $10,000 from a tabloid [newspaper] to read those e-mails and spy on Chelsea for whatever reason," he said.

Sensitive corporate information and trade secrets are equally vulnerable when they are mentioned in e-mail, which has its roots in an easy-to-read format.

"If anything cried out for being encrypted, I would say e-mail does," Smith said. "Maybe over time, that can be a change that happens."

Actually, powerful encryption tools are currently available to virtually all computer users, though they take some knowledge of computers to properly employ.

Computer experts foresee growing consumer demand for encryption. "We can expect that as people learn that e-mail is not secure, there'll be more interest in using encryption to protect it," said Matt Blaze, a research scientist with AT&T Labs. "Most people now don't use it because they're not interested in it or it's not available to them in the standard configuration that comes with their computer."

Perrine said an Internet engineering standards group recently developed guidelines that could hasten the day when people routinely send encrypted e-mail messages.

"All traffic between cooperating computers would be encrypted and in most cases this would be transparent to the user," he said. "Those technologies, if they're not already here, are at least on the horizon."

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

Copyright 2000 Michigan Daily via U-Wire
University Wire

July 25, 2000

SECTION: EDITORIAL
LENGTH: 601 words
HEADLINE: E-mail's big brother
BYLINE: Staff Editorial, Michigan Daily
SOURCE: U. Michigan
DATELINE: Ann Arbor, Mich.
BODY:

The FBI has recently come under fire from internet privacy groups and the ACLU for a controversial e-mail snooping system that monitors all e-mail passing through networks connected to the device. The system, dubbed "Carnivore" by the FBI -- because it gets at the "meat" of information -- is dangerous because it is capable of scanning sender and receiver information along with the subject lines of all passing mail to determine if those messages contain information worth saving for FBI review. Unlike phone taps, Carnivore's almost unlimited access to private messages carries a high potential for abuse by overzealous FBI agents and allows the possibility of targeting users not suspected of any crime.

Court orders are currently required to tap phone lines or gather information from ISP's on possible illegal activity carried out over electronic mediums like e-mail, but Carnivore is much more pervasive. The system is an untouchable box installed on private networks to collect all information passing through them. This is like installing a device that listens to every phone conversation to determine whether or not the phone calls should be monitored by law enforcement. But information on the inner workings of Carnivore remains sketchy. This alarms many privacy advocates, like Representative Bob Barr (R-GA), who had one word for the system: "Frightening."

One solution involves allowing the code of Carnivore to be perused by independent groups who would examine its workings to make sure the information being collected is limited to those under investigation for illegal activity. This seems a viable solution, as the integrity of the Carnivore system would not be violated, yet could still be monitored. The FBI announced Friday that Carnivore could be reviewed by independent academics, but this does not go far enough.

A more palatable alternative to Carnivore would leave ISP's responsible for turning over information on targeted users for FBI review, as is the current practice with phone companies in possession of incriminating evidence. This allows some degree of protection and would be a reasonable alternative to widespread electronic surveillance.

More sweeping reform could come from Congress, as legislators examine the ACLU's recommendation to draft legislation that would bring Carnivore and similar schemes under control. Current privacy legislation needs to evolve to include provisions ensuring that access to electronic communications by law enforcement is limited to suspect users and specific court-approved targets only. The potentially abusive nature of Carnivore is not something we should learn to live with in the digital age. Law-abiding citizens cannot have their privacy infringed by law enforcement agencies interested in collecting data on a few criminals.

Congress must keep up with the times and fully examine the feasibility of wide-ranging changes to electronic privacy. Outdated laws like the 14-year-old Electronic Communications Privacy Act, which allows for real-time interception of messages with a court order, does not include provisions for new technologies and allows for loopholes like Carnivore.

Doc. #41

Whether Carnivore's code is opened to public investigation or more stringent attention is paid to governmental bodies engaged in electronic snooping, the laws are far behind technological means. It is time the American people receive comprehensive legislative protection from risky, unaccountable law enforcement techniques that violate Fourth Amendment protection from unreasonable searches.

(C) 2000 Michigan Daily via U-WIRE

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

Copyright 2000 The Washington Post
The Washington Post

July 25, 2000, Tuesday, Final Edition

SECTION: FINANCIAL; Pg. E01
LENGTH: 704 words
HEADLINE: FBI Makes Case For Net Wiretaps; 'Carnivore' System Faces Fire on Hill
BYLINE: John Schwartz , Washington Post Staff Writer
BODY:

Federal law enforcement officials defended "Carnivore"--the FBI's controversial Internet wiretap system--through more than two acrimonious hours of grilling by Democratic and Republican lawmakers yesterday, painting a chilling picture of an Internet that would become a safe haven for crooks and terrorists without proper surveillance.

"Criminals use computers to send child pornography to each other using anonymous, encrypted communications," FBI Assistant Director Donald M. Kerr told the House Judiciary subcommittee on the Constitution. "Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet."

Many of the lawmakers seemed just as concerned with the actions of the law enforcement officials. "The potential for abuse here is tremendous," said Rep. Spencer Bachus (R-Ala.). "What you're saying is 'Trust us.' "

Carnivore is a modified version of a common network-maintenance program known as a "packet sniffer." Carnivore offers great specificity--the ability to quickly collect just the "to" and "from" information in e-mail messages, for example, and not online banking transactions. That gives law enforcement the equivalent of the telephone world's "pen register" and "trap and trace" data--the origin and destination of all calls related to the subject.

Civil liberties groups and Internet service providers say the system raises troubling questions about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, they note, the new technology also could scan private information about legal activities, taking in vast amounts of information from innocent people as well as the suspect.

The critics also note that past experience has shown that law enforcement has overstepped its wiretap authority numerous times in the past.

Barry Steinhardt, associate director of the American Civil Liberties Union, said in his testimony: "Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target."

Officials of Internet service providers who oppose the technology say they are wary of putting equipment designed by others on their networks. They want the FBI to publish information on the software used so that ISPs can be sure that it does what the agency says.

The law enforcement officials pledged to present the system to a neutral third party for review but said they cannot release so much information about the system that it will become a target for evasion and hacking.

They insisted the Carnivore system actually provides greater privacy than previous methods of gathering electronic information because it can fine-tune what the machine hands over to investigators.

DOC. #42

The FBI's Kerr also argued that agents won't "risk their integrity, their jobs and their futures" by abusing the law.

The toughest questioning came from Reps. Jerrold Nadler (D-N.Y.) and Robert L. Barr Jr. (R-Ga.), two congressmen rarely on the same side of an issue. Nadler peppered the officials with a series of questions that underscored the point that Carnivore, under the laws that govern pen-register surveillance, could be used without the difficult showing of "probable cause" required in a telephone wiretap.

Barr cited the investigation of missing White House e-mail and scornfully said the Clinton administration asserts that "we don't even know how to keep track of our own e-mail" while "now we see a very sophisticated system for keeping track of other people's e-mails!"

After the hearing, House Majority Leader Richard K. Armey issued a statement saying members of both parties showed "strong concerns that the administration is infringing on Americans' basic constitutional protection against unwarranted search and seizure.

"Until these concerns are addressed," he concluded, "Carnivore should be shut down."

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

Copyright 2000 News World Communications, Inc.
The Washington Times
July 25, 2000, Tuesday, Final Edition

SECTION: PART A; Pg. A1
LENGTH: 744 words
HEADLINE: Lawmakers rip FBI e-mail tracker;
Surveillance tool employed 25 times
BYLINE: William Glanz; THE WASHINGTON TIMES
BODY:

Federal law enforcement agents say they have used the controversial Carnivore software program to track e-mail of suspects 25 times in the past two years.

But agents have never used the program illegally or tracked e-mail they were not authorized to track by a court order, FBI Assistant Director Donald Kerr told the House Judiciary subcommittee on the Constitution yesterday.

Despite the restraint the FBI says it has used, privacy rights advocates criticized law enforcement agents for using Carnivore and lawmakers expressed skepticism about the federal government's use of the Internet surveillance tool.

House Majority Leader Dick Armey, Texas Republican, said yesterday Carnivore should be suspended until concerns of privacy advocates and needs of law enforcement are reconciled.

"Until these concerns are addressed, Carnivore should be shut down," he said.

Carnivore enables investigators to pick out specific e-mail messages traveling through an Internet service provider's computer system so it can monitor who a suspect contacts and who contacts a suspect.

Mr. Kerr and other federal officials said the high-tech surveillance system is crucial to help them keep up with an increasingly sophisticated breed of tech-savvy criminals and crucial to help them keep the Internet safe.

"Many of the crimes that we confront every day in the physical world are beginning to appear on line," said Deputy Assistant Attorney General Kevin DiGregory.

"If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the information age. . . . Carnivore is simply an investigative tool that is used on line only under narrowly defined circumstances and only when authorized by law to meet our responsibilities to the public," he said.

But lawmakers expressed concern about a lack of checks and balances on law enforcement agents using Carnivore.

"The potential for abuse here is enormous," said Rep. Spencer Bachus, Alabama Republican.

FBI General Counsel Larry Parkinson said Carnivore is a little-used tool. When it is used, Mr. Kerr said, agents follow the law carefully, and if they are caught collecting more data than allowed, they can be imprisoned up to five years for committing a federal felony.

"In the past, we've had many agencies go beyond the scope of their authority," said Rep. John Conyers Jr., Michigan Democrat.

Mr. Kerr said the FBI and Department of Justice will seek an independent

Doc. #43

review of Carnivore this year to show they aren't misusing the program.

Lawmakers and privacy rights advocates also criticized federal officials for using Carnivore when Internet service providers could just as easily collect information being sought.

"There ought to be more control in the hands of the Internet service providers ," said Alan Davidson, a lawyer with the District-based civil liberties group Center for Democracy and Technology.

Mr. Kerr argued that few of the nation's estimated 10,000 Internet service providers have the means to sift through e-mail traffic and collect them for law enforcement.

But Robert Corn-Revere, an attorney who represented Atlanta-based Internet service provider EarthLink, said EarthLink was gathering e-mail information at the federal government's request earlier this year when it was forced to comply with a court order and let federal officials install Carnivore on its computers.

The federal government was upset that EarthLink was capturing few e-mail messages, Mr. Corn-Revere said, and it needlessly installed Carnivore.

American Civil Liberties Union Associate Director Barry Steinhardt suggested Carnivore's source code be made public. The source code is the set of instructions a programmer writes, and it will show just what Carnivore is capable of retrieving. The ACLU has filed a Freedom of Information Act request with the FBI to get the source code.

Even though they had a raft of questions about Carnivore and its use, lawmakers yesterday didn't express any willingness to make immediate changes in the federal government's authority to use the surveillance program.

"We should be sensitive to any potential for abuse of the Carnivore system. Even a system designed with the best of intentions to legally carry out essential law enforcement functions may be a cause for concern if its use is not properly monitored," said Rep. Charles T. Canady, Florida Republican.

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

Copyright 2000 Burrelle's Information Services
CBS News Transcripts

SHOW: CBS MORNING NEWS (6:30 AM ET)
July 25, 2000, Tuesday

TYPE: Newscast
LENGTH: 388 words
HEADLINE: NEW SURVEILLANCE SOFTWARE ALLOWS THE FBI TO SNOOP THROUGH COMPUTER USERS' E-MAILS
ANCHORS: SHARYL ATTKISSON
REPORTERS: JIM STEWART
BODY:

SHARYL ATTKISSON, anchor:

First came wiretapping phones. Now the FBI is using a controversial cybersurveillance program called Carnivore that wiretaps the Internet. Jim Stewart reports.

JIM STEWART reporting:

Every day, more than a billion e-mails are sent and received by computer users, and the FBI thinks criminals are now just as fond of them as the next guy. But the problem for agents has always been: Just how do you sort through all the gibberish to find any meaningful evidence? The bureau told Congress it thinks it's found the answer in a software program called Carnivore.

Mr. LARRY PARKINSON (General Counsel, FBI): This is--despite its unfortunate name, this is a tool that is very surgical.

STEWART: Essentially, Carnivore is like a wiretap on the Web. Physically, it's nothing more than a small computer the FBI can lock inside the switching room of an Internet service provider like, say, America Online. But instead of reading every AOL customer's e-mail, it's designed to zero in and record just the messages sent to and from one particular e-mail address.

Mr. DONALD KERR (Director, Lab Division, FBI): We don't do broad searches or surveillance with this system. That's not authorized by a court order and, in my view, could not be.

STEWART: Critics, however, immediately asked: Who's watching the watchers?

Mr. ALAN DAVIDSON (Center for Democracy & Technology): Carnivore has access to much more information than it is legally entitled to collect. How do we know that we can trust Carnivore? How do we know what kind of leash has been put on Carnivore?

STEWART: The reason for the skepticism is because there's a big difference between wiretapping the Internet and wiretapping a telephone. If the FBI wants to bug your telephone, they get a court order and go to the phone company, and the phone company makes the connection for the bureau. If the FBI wants to wiretap your Internet address, they get a court order and then they can make the connection themselves.

They've done it 16 times this year already, mostly against Internet hackers, and the potential list of suspects and their crimes is growing, agents warned. Four years from now, the number of commercial e-mail messages alone is expected to top 200 billion a year. Jim Stewart, CBS News, Washington.

LANGUAGE: English

LOAD-DATE: July 25, 2000

Doc. #44

Copyright 2000 Seattle Post-Intelligencer
SEATTLE POST-INTELLIGENCER

July 25, 2000, Tuesday

SECTION: NEWS,
LENGTH: 664 words
HEADLINE: FBI ACCUSED OF VIOLATING E-MAIL PRIVACY;
ADVOCATES SAY PROGRAM SIFTS THROUGH EVERY FILE SENT THROUGH SPECIFIC ISPMARK
HELM P-I WASHINGTON BUREAU
DATELINE: WASHINGTON
BODY:

Privacy advocates and technology experts yesterday blasted a new FBI program to police the Internet, saying the system allows agents to monitor e-mails of people who are not targets of criminal investigations.

"The FBI asks you to trust them with unsupervised access . . . to literally millions of innocent communications," Barry Steinhardt, associate director of the American Civil Liberties Union, told a House subcommittee investigating the system. "For me, that's an enormous leap of faith that the public is being asked to take."

The e-mail sniffing system, known as "Carnivore," allows law enforcement officials to sift a suspect's messages out of the full stream of data passing through an Internet service provider (ISP), like America Online.

Once installed on the ISP network, Carnivore can monitor all of the e-mail on that ISP, from the list of what is sent to the actual content of the e-mail.

Steinhardt told the subcommittee on the Constitution that Carnivore differs significantly from traditional phone wiretaps. With a phone wiretap, the FBI must obtain a court order to monitor conversations of a specific phone. Then, the FBI contacts the phone company, which installs the tap, and, when the investigation ends, disconnects it. Agents are not able to monitor any conversations other than those on the one phone.

Under the Carnivore system, the FBI first gets a court order to use the agency's software to tap into the lines of an ISP. Unlike a traditional wiretap with access to only one phone, Carnivore has access to every message being sent along the ISP's system. In addition, the ISP has no control over or knowledge of what the FBI is monitoring.

Peter Sachs, president of ICONN, a New Haven, Conn.-based ISP, said Carnivore violates the rights of every "law-abiding" citizen who uses the Internet to send e-mail.

"At this very moment, a government-controlled computer, installed under court order at some ISP somewhere in this country is busy reviewing all communications passing through that ISP, including messages from and to you, the members of Congress."

Sachs said the software used for Carnivore, which is secret, also poses other threats to Internet users. First, he said, the software could be vulnerable to hackers. Another problem, he said, is that the Carnivore already has caused service problems for several ISPs, causing them to stop or slow down.

But Justice Department and FBI officials said they are simply trying to preserve their ability to monitor criminal activity. They said that capability is being eroded by the growing use of new technologies such as encryption, cell phones and wireless message devices.

Kevin DiGregory, deputy associate attorney general, said Carnivore actually protects privacy because it can be configured to identify only the senders and

Doc. #45

recipients of the suspect's e-mail. The system selects only the data related to the criminal suspect, he said, so that human reviewers see only what the machine has culled.

"It's not just a situation where, as I understand it, a rogue FBI agent, for example, could broaden the coverage of the Carnivore intercept and violate the court order," DiGregory said. "In order to do that, he would need to engage the aid of technical people, perhaps even technical people at the Internet service provider."

Donald Kerr, director of the FBI's computer lab division, said Carnivore is used only when an ISP cannot provide the information requested under a court order. "The FBI would prefer to let ISPs do this work, but sometimes that's not possible and in those cases, we bring in Carnivore," he said.

Existing laws are ambiguous about what standards apply for different kinds of Internet surveillance.

Last Monday, the White House announced the administration will propose legislation to "harmonize" the laws of wiretapping as it affects the many technologies by which people communicate - such as telephone, dial-up modem and high-speed broadband access.

LANGUAGE: ENGLISH

LOAD-DATE: July 26, 2000

Copyright 2000 Post-Newsweek Business Information, Inc.
Newsbytes

July 27, 2000, Thursday

LENGTH: 481 words

HEADLINE: GOP Lawmakers Want To Starve "Carnivore"

BYLINE: David McGuire; Newsbytes

DATELINE: WASHINGTON, D.C., U.S.A.

BODY:

A powerful cadre of House Republicans today demanded that the FBI pull the plug on its controversial e-mail surveillance device, "Carnivore."

"Given the uproar Carnivore has created, and the potential impact reports on Carnivore could have on consumer confidence in the Internet, we urge you to suspend any activity involving the development or use of Carnivore until the serious privacy issues involved have been satisfactorily answered," the lawmakers wrote in a sternly worded letter to Attorney General Janet Reno.

Signed by 27 House Republicans including Majority Leader Dick Armey, R-Texas, and Majority Whip Tom DeLay, R-Texas, today's letter is aimed at forcing the Justice Department to move quickly in addressing the constitutional concerns raised by the FBI's use of the controversial device, Armey staffer Richard Diamond told Newsbytes today.

Designed to attach directly to an Internet service provider's internal systems, Carnivore is capable of sifting through vast quantities of e-mail messages to find those that meet investigative specifications of a court order. Messages that don't meet the specific parameters of a given court order are - according to the FBI - never read.

But the revelation that the FBI is sifting through millions of innocent Internet users' e-mail messages has spawned a groundswell of opposition to the device. Conservatives and liberals alike have decried the FBI's use of the device, claiming that using the technology violates constitutionally protected privacy rights.

"You shouldn't be using this kind of (technology) with this type of question hanging over your head," Diamond said.

The authors of today's letter asked Reno to retire the device until the FBI and Justice Department can adequately address the privacy concerns it raises. However, Reno, in her weekly Justice Department news briefing, said she would not suspend use of the device until after an internal FBI review of Carnivore is completed.

Diamond conceded that it is probably unlikely that Carnivore would ever meet with congressional approval. "The burden of proof is on the Attorney General to show us that (Carnivore) is in full compliance with the Fourth Amendment," Diamond said.

And at least one signatory to today's letter doesn't intend to wait for the Justice Department to shelve Carnivore of its own volition.

Rep. Bob Barr, R-Ga., is crafting legislation that would prevent the FBI from using Carnivore and devices like it, Barr staffer Brad Alexander said today.

The Justice Department was not available for comment on today's letter.

Doc. # 46

Earlier this month, Reno promised to personally investigate the FBI's use of Carnivore.

Reported by Newsbytes.com, http://www.newsbytes.com .

16:31 CST Reposted 16:31 CST

(20000727/WIRES ONLINE, LEGAL, BUSINESS/FBI/PHOTO)

LANGUAGE: ENGLISH

TYPE: NEWS

LOAD-DATE: July 28, 2000

Copyright 2000 Post-Newsweek Business Information, Inc.
Newsbytes

July 27, 2000, Thursday

LENGTH: 516 words

HEADLINE: Privacy Legislation Won't Move This Year - Leahy

BYLINE: David McGuire; Newsbytes

DATELINE: WASHINGTON, D.C., U.S.A.

BODY:

While broad-based Internet privacy legislation probably won't go very far in this congressional session, lawmakers are making progress on the thorny issue and will ideally be ready to develop something substantive next year, Sen. Patrick Leahy, D-Vt., told reporters and high- tech industry leaders today.

"I don't think anything will be done significantly this year," Leahy said, adding that Congress should begin working in earnest on setting baseline federal privacy standards next year, after the presidential election brouhaha has a chance to die down.

Despite the difficulty of establishing substantive privacy legislation in this Congress, Leahy blasted the notion of punting the privacy issue to a congressionally appointed panel.

"If we've got time to investigate the investigations of (Clinton Administration scandals) we ought to at least find the time to do something real-world" on privacy, Leahy said.

Pending House legislation would establish a commission to delve into the Internet privacy issue.

Although industry leaders remain leery of accepting federal Internet privacy standards without a fight, the business community's growing willingness to at least discuss a legislative remedy should help clear the way to enacting privacy legislation, Leahy said.

Leahy spoke today at a breakfast meeting on Capitol Hill where the Business Software Alliance (BSA) honored him with a "Cyber Champion Award." BSA, which represents a slew of large software makers - including Microsoft Corp. - doles out the Cyber Champion statuettes to lawmakers and regulators who support intellectual property and anti-piracy causes.

In addition to his work in the privacy arena, Leahy has played key roles in combating software piracy and supporting the relaxation of US export controls on encryption products. BSA leaders said that they gave Leahy the award to thank him for his work in those areas.

Following the meeting, BSA president Robert Holleyman told Newsbytes that while the software industry does not openly endorse the creation of federal privacy standards, the group would be open to discussing limited legislation with Leahy and his colleagues next year.

"It is premature to do something in Congress this year," Holleyman said. But BSA and its member companies would be willing to talk about endorsing strictly limited federal privacy legislation - particularly if such legislation would preempt harsher state and local measures.

Still, BSA wants Congress to give industry self-regulation a chance and

Doc. #47

Holleyman remains concerned that any privacy bill may go too far for his taste.

"Something might get started in that process that just becomes a snowball," Holleyman said.

During his remarks today, Leahy also addressed "Carnivore," the FBI's controversial e-mail surveillance device. "I don't think we are doing adequate oversight on Carnivore," Leahy said.

Reported by Newsbytes.com, http://www.newsbytes.com .

14:15 CST

(20000727 /WIRES ONLINE, LEGAL, BUSINESS/PRIVACYDOME/PHOTO)

LANGUAGE: ENGLISH

TYPE: NEWS

LOAD-DATE: July 27, 2000

Copyright 2000 The New York Times Company
The New York Times

July 27, 2000, Thursday, Late Edition - Final

SECTION: Section A; Page 24; Column 1; Editorial Desk

LENGTH: 635 words

HEADLINE: Wiretapping in Cyberspace

BODY:

Millions of Americans now log on to the Internet as naturally and as frequently as they pick up a phone. Technology has created a revolution in personal communications, but technology is also making it possible for government and even employers to monitor private conversations as never before. Telephone-era laws must be updated to address these new challenges to privacy.

Last week the White House proposed some limited changes to the federal wiretap and electronic privacy laws that would raise legal standards for government interception of e-mail. Separately, several lawmakers introduced legislation to require employers to notify employees about how e-mail, Internet use and phone calls are monitored. Employees of The New York Times Company are already notified that the company reserves the right to review e-mail messages while investigating a complaint. Last year the company dismissed 23 employees -- most based at a regional business office -- for sending offensive e-mail messages.

In the absence of more stringent controls, law enforcement agencies may be tempted to conduct wholesale monitoring of digital written communications. It is probably not practical for agents to listen in on all the phone calls, for example, that go through AT&T. But new technology is making it possible for agencies like the F.B.I. to scan, read and record millions of pieces of e-mail on the network of an Internet service provider. Until now, this kind of power and its potential for abuse were not so readily available.

Current wiretapping laws were not drafted with this technology in mind and need to be updated. Various statutes now set different legal standards for the secret interception of domestic communications by law enforcement agencies, depending on whether the communication is by telephone, e-mail or cable modem.

The Clinton administration is proposing to eliminate these inconsistencies. Its plan would bring the standards used for intercepting e-mail messages up to the stricter, more protective level now applied to telephone wiretaps. Illegal interception of e-mail would result in suppression of the evidence, as is the case now with illegal interception of phone calls. The proposal would also enforce the same legal standards that apply to phone calls for interception of e-mails sent by cable modems, which have a greater degree of privacy protection under a law that governs cable systems.

The administration is also calling for greater authority for courts to review law enforcement requests to use devices that record the phone numbers of incoming and outgoing calls and to track the origins and destinations of e-mail messages.

These changes are clearly needed. But Congress also needs to provide new safeguards against the government's wrongful use of ever more powerful surveillance technology against law-abiding citizens. Serious concerns have been raised about Carnivore, the new online wiretap system used by the F.B.I.

DOC. #48

to track the communications of individuals suspected of criminal activity.

The F.B.I. says the technology can isolate the e-mail of the target of an investigation. But the system, when hooked up to the network of the Internet service provider, gives the F.B.I. unlimited access to the e-mail of all other subscribers on the network. While a court order is still required to intercept the content of messages, the secret technology controlled exclusively by law enforcement raises fears of improper monitoring.

Until now, routine government surveillance of private conversations was limited as much by practicality as by legal constraints. Now that it is feasible to eavesdrop electronically on an unlimited scale, the laws have to be strengthened to prevent monitoring of all online communications simply because technology makes it easy.

http://www.nytimes.com

LANGUAGE: ENGLISH

LOAD-DATE: July 27, 2000

Copyright 2000 eMediaMillWorks, Inc.

(f/k/a Federal Document Clearing House, Inc.)
Congressional Press Releases

July 27, 2000, Thursday

SECTION: PRESS RELEASE
LENGTH: 478 words
HEADLINE: REP. CANADY INTRODUCES BILL TO UPDATE WIRETAP LAWS
BYLINE: CHARLES T. CANADY , REPRESENTATIVE , HOUSE

BODY: For immediate Release July 27, 2000 Rep. Canady Introduces Bill to Update Wiretap Laws E-Mails and Stored Internet Communications Would Be Covered WASHINGTON, D. C. - Rep. Charles T. Canady (R-FL), Chairman of the House Judiciary Subcommittee on the Constitution, today introduced the Electronic Communications Privacy Act of 2000. The bill would update the federal wiretap laws to cover e-mail and stored electronic communications, as well as provide special requirements for government tracing of e-mail addresses. Canady is joined by original cosponsor Rep. Asa Hutchinson (R-AR). "This legislation helps move our federal wiretap laws into the 21st Century," Canady said. "We have entered a new age with the Internet, and we need a new law to reflect the rapid changes in technology. While this legislation does not answer all the difficult issues raised by recent technological advances, it does provide for some reasonable reforms that will protect the privacy rights of Americans." Earlier this week, Rep. Canady chaired a Constitution Subcommittee hearing on Fourth Amendment issues raised by the FBI's "Carnivore 11 program. The FBI designed and developed Carnivore to isolate, intercept and collect communications that are the subject of lawful court orders. The July 24th hearing featured witnesses from law enforcement, civil liberty organizations, privacy organizations and representatives from the business community. BILL SUMMARY The Electronic Communications Privacy Act of 2000 has three sections. The first section amends the "statutory exclusionary rule" to also exclude from use as evidence illegally intercepted "electronic communications" and illegally obtained "stored electronic communications."

The bill simply adds electronic communications to the previously covered wire and oral communications. The second section of the bill requires the federal government to produce annual reports regarding its requests for orders for the disclosure of "stored electronic communications." This reflects virtually identical disclosure requirements the federal government must meet regarding the use of electronic wiretaps. The final section of the legislation amends the definition of "pen register" and "trap and trace" devices, defining them to allow the identification of an "e -mail address." In addition, the section requires that, if a pen register or trap and trace device is used to identify an e-mail address, the federal government must first demonstrate to a court that "specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use (of a pen register or trap and trace device) is relevant to an investigation of that crime." For a copy of Rep. Canady's legislation (7pages) please call Michelle Knott at (202) 22-5-1252.

LANGUAGE: ENGLISH
LOAD-DATE: July 31, 2000, Monday

Copyright 2000 Copley News Service

Copley News Service

July 27, 2000, Thursday

SECTION: Commentary

LENGTH: 396 words

Doc. #49

HEADLINE: Gobbling G-men

BODY:

It's ironic that the company the Justice Department worked so hard to break up is crumbling cookies while the government is eating raw meat.

Cookies, as many computer users know, are bits of code that help Web sites keep track of visitors. In addition to innocent uses, cookies have been exploited by hucksters to learn consumers' interests and habits without their knowledge. They're an immeasurable source of personal information.

So, it was welcome news recently when Microsoft Corp. announced new software to allow the individual user to block some or all of these tempting little tastes of their private lives.

In the news about the same time was the FBI's revelation that for the past 18 months it has been using a computer program called Carnivore, which when installed on the network of an Internet provider can comb millions of e-mail messages. The potential for mischief makes cookies seem like something from Grandma's oven.

This new first cousin to wiretapping is necessary, the FBI says, to keep up with ever-more-sophisticated drug dealers and other criminals.

The question is, how do we make sure the authorities are riffling through cybercorrespondence from actual or probable crooks and not the e-files of innocent citizens, members of unpopular groups or political enemies of someone in power?

Pressed by lawmakers, civil libertarians and privacy advocates, the Clinton administration has promised to develop guidelines for bringing consistency and control to e-mail surveillance. (Is there a chance Vice President Al Gore's missing fund-raising e-mails might turn up in the process?)

A major sticking point is the degree of say that Internet providers, standing in for their customers, would have. Clearly, the FBI would prefer to monitor e-mail traffic, with court permission, on its own terms with its own filtration. Privacy groups and some of the providers suggest instead that the feds obtain a court order asking the companies for specific material on a case-by-case basis.

Sounds reasonable. Justifying intrusion prior to the intrusion would not hobble law enforcement and would reassure the overwhelming majority who use the Internet without criminal intent that a large Carnivore was not following their trail of cookie crumbs.

Reprinted from the Indianapolis Star.

SMOLAN-CNS-SD-07-27-00 0703PST
LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

Copyright 2000 Post-Newsweek Business Information, Inc.
Newsbytes

July 28, 2000, Friday

LENGTH: 473 words

HEADLINE: Barr Introduces Legislation To Kill Carnivore

BYLINE: David McGuire; Newsbytes

DATELINE: WASHINGTON, D.C., U.S.A.

BODY:

Hoping to permanently pull the plug on the FBI's controversial e-mail surveillance device, Carnivore, Rep. Bob Barr, R-Ga., on Thursday introduced legislation that would curtail law enforcers' rights to monitor the activity of Internet users.

As he promised earlier this week, Barr introduced the Digital Privacy Act of 2000, which updates federal wiretapping laws to "bring them in line with technological developments such as the Internet, wireless phones and electronic mail," Barr's office said in a statement today.

Specifically, the legislation would prevent the FBI and other law enforcers from accessing individuals' computer files unless "factual evidence reasonably indicates that a crime has been, is being or will be committed."

Electronic evidence illegally obtained by law enforcers would be barred from use in court under the legislation.

Barr's legislation is the latest and most tangible attack on Carnivore, which has been drawing broad-based criticism since news of its use was made public earlier this month.

Designed to attach directly to an Internet service provider's internal systems, Carnivore is capable of sifting through vast quantities of e-mail messages to find those that meet investigative specifications of a court order. Messages that don't meet the specific parameters of a given court order - according to the FBI - are never read.

But the revelation that the FBI is sifting through millions of innocent Internet users' e-mail messages has spawned a groundswell of opposition to the device. Conservatives and liberals alike have decried the FBI's use of the device, claiming that using the technology violates constitutionally protected privacy rights.

Under Barr's legislation, the FBI would not be able to sift through the messages of innocent e-mail users in search of criminal evidence.

One of Carnivore's most ardent congressional opponents, Barr on Thursday was one of more than 25 lawmakers who signed a letter to Attorney General Janet Reno demanding that the FBI shelve the device until the constitutional issues surrounding its use are resolved.

"Given the uproar Carnivore has created, and the potential impact reports on Carnivore could have on consumer confidence in the Internet, we urge you to suspend any activity involving the development or use of Carnivore until the serious privacy issues involved have been satisfactorily answered," the lawmakers wrote.

In addition to hamstringing unchecked e-mail surveillance, Barr's legislation would also prevent law enforcers from tracking the movements of

Doc. #50

cell phone users without first obtaining a court order.

Reported by Newsbytes.com, http://www.newsbytes.com .

16:49 CST Reposted 16:52 CST

(20000728/WIRES ONLINE, LEGAL, BUSINESS/PRIVACYDOME/PHOTO)

LANGUAGE: ENGLISH

TYPE: NEWS

LOAD-DATE: July 29, 2000

Copyright 2000 The News and Observer
The News and Observer (Raleigh, NC)

July 28, 2000 Friday,

STATE EDITION

SECTION: NEWS;

Pg. A7;

NATIONAL BRIEFS

LENGTH: 132 words

HEADLINE: Reno won't suspend 'Carnivore' just yet

BYLINE: From Wire Reports

BODY:

Washington, D.C. -- Attorney General Janet Reno said Thursday she will not suspend the FBI's court-approved monitoring of some people's e-mail while the law enforcement program is under review at the Justice Department. "I think that (FBI) agents can still use it" during the review of the FBI's new "Carnivore" system, Reno said at her weekly news briefing.

Reno said it is important "that we be able to explain the process and address the issues raised by the industry, privacy experts and others." She said she hopes "we will be able to address these issues in a thoughtful way and resolve them."

Reno's comments came amid a move in Congress to increase the burden on federal law enforcement agencies to justify monitoring e-mail and other communications.

LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

DOC. #51

Copyright 2000 National Journal Group, Inc.
National Journal's Technology Daily

PM Edition

July 28, 2000

LENGTH: 238 words

HEADLINE: PRIVACY: Barr To Introduce Digital Privacy Act

BYLINE: Drew Clark

BODY:

Rep. Bob Barr, R-GA, said Friday he would introduce legislation dubbed the Digital Privacy Act that would update wiretapping laws to enhance privacy protections by restricting the police's ability to obtain surveillance information with a warrant issued by a judge.

One provision of the legislation that is similar to a proposal by Sen. Patrick Leahy, D-VT, would give judges discretion over whether or not to authorize wiretaps.

Currently, judges must approve such requests so long as a law enforcement officer swears that it is relevant to an ongoing investigation.

Another provision of the bill would overrule a controversial decision last year by the Federal Communications Commission and would stop the government from tracking the location of cell phone users without a court order. "As the White House recently acknowledged, our wiretapping laws have fallen far behind the technological explosion of the past decade," said Barr, a former CIA agent and federal prosecutor. "The Digital Privacy Act corrects some of the most glaring contradictions and loopholes in current law.

As systems from NSA's Echelon spy project to FBI's Carnivore have proven, technological advances make large-scale surveillance easier than ever before. It is vital we safeguard our civil liberties by making certain the law changes to prevent longstanding Fourth Amendment protections from being eroded," Barr said.

LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

Doc. #52

Copyright 2000 CNBC, Inc.
Copyright 2000 eMediaMillWorks, Inc.

(f/k/a Federal Document Clearing House, Inc.)
Congressional Press Releases

July 28, 2000, Friday

SECTION: PRESS RELEASE

LENGTH: 301 words

HEADLINE: BARR BILL UPDATES WIRETAP LAWS

BYLINE: BOB BARR , REPRESENTATIVE , SENATE

BODY: FOR IMMEDIATE RELEASE JULY 27, 20000 BARR BILL UPDATES WIRETAP LAWS MEASURE ENHANCES ELECTRONIC PRIVACY PROTECTION WASHINGTON, D.C. -- U.S. Representative Bob Barr (GA-7) announced today he was introducing the "Digital Privacy Act of 2000." The legislation updates wiretapping laws to enhance privacy protections and bring them in line with technological developments, such as the Internet, wireless phones, and electronic mail.

Specifically, the measure would: > Extend reporting statues requiring law enforcement to report on its interception of electronic communications, in addition to the telephone wiretap reports already required. > Block the use of electronic evidence in court if it is obtained illegally. > Stop unchecked government access to the identities of computer users unless there is reasonable evidence a crime has been committed. > Stop the government from tracking the location of cell phone users without a court order based on probable cause. "As the White House recently acknowledged, our wiretapping laws have fallen far behind the technological explosion of the past decade. For example, under current law, e-mails receive less legal protection than both traditional postal mail and telephone conversations," said Barr. "The Digital Privacy Act corrects some of the most glaring contradictions and loopholes in current law. As systems from NSA's Project Echelon to FBI's Carnivore have proven, technological advances make large scale surveillance easier than ever before. It is vital we safeguard our civil liberties by making certain the law changes to prevent longstanding Fourth Amendment protections from being eroded," Barr continued. Barr, a Member of the House Judiciary Committee, has served with both the Department of Justice and the Central Intelligence Agency.

LANGUAGE: ENGLISH

LOAD-DATE: July 31, 2000, Monday

Doc. #53

Copyright 2000 The Denver Post Corporation
The Denver Post

July 28, 2000 Friday

2D EDITION

SECTION: BUSINESS;

Pg. C-04

LENGTH: 867 words

HEADLINE: Soaring online warrants worry privacy advocates

BYLINE: By Will Rodger, USA Today.com,

BODY:

The number of search warrants seeking citizens' online data has soared during the past few years, a USA Today.com study shows.

The findings, based on an examination of search warrants served on the nation's largest Internet service provider, America Online, came as a surprise to federal lawmakers and civil libertarians and are prompting calls for legal reforms.

800 percent jump

The warrants, served by state and local investigators from across the nation, were aimed at discovering the identity and activities of AOL subscribers. In 1997, AOL was served with 33 search warrants, according to court logs in Loudoun County, Va., where AOL is based. That number jumped to 167 in 1998 and 301 in 1999 - an increase of more than 800 percent.

This year, state and local investigators had served 191 warrants on AOL through July 17, the logs show.

Congressional leaders informed of USA Today.com's findings said they will examine legal standards applied to Internet investigations. At a minimum, House Majority Leader Dick Armey, R-Texas, said police need to tell Congress when, why and how they perform electronic searches.

Critics are concerned because they believe that electronic surveillance of all types is a highly powerful tool that, if not tightly controlled, violates rules against unreasonable police searches.

'We do have reports on wiretaps,' Armey said. 'Why shouldn't people have a right to know what the government is doing to access personal correspondence in any media?'

Armey's displeasure echoes the criticism members of a House subcommittee expressed this week about the FBI's new 'Carnivore' Internet wiretapping device. Some say the FBI may be intercepting too much e-mail when it tries to nab messages still in transit from one Net user to another.

But privacy advocates say that while official Washington occupies itself with the legality of Carnivore's real-time e-mail interception, it is ignoring another, possibly more important point: The e-mail stored in online accounts after messages have been delivered has only a fraction of the protections afforded an ordinary telephone call or e-mail still in transit.

Searches for online data typically involve cases ranging from harassment and child pornography to violent crime and fraud.

Doc. #54

White House chief of staff John Podesta has pledged the administration would move soon to protect electronic data.

'Data transmitted over networks is not afforded the full privacy protection we give to traditional phone calls,' he said. 'Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information, shouldn't they count, as (U.S. Supreme Court Justice) Louis Brandeis foreshadowed more than 70 years ago, as the papers and effects mentioned in the Fourth Amendment?'

FBI downplays concerns

FBI officials say there is little reason for concern that stored e-mail and other online records are not as confidential as a personal telephone call.

FBI assistant general counsel Thomas Gregory Motta said the law has treated stored records like e-mail the same way it handles other documents such as letters and diaries, which can be seized from a home with a simple search warrant. 'What about records of my transactions at a bank?' he said. 'I can get that with a subpoena from a grand jury.'

What authorities are looking for can vary by case. In some instances, the logs show, police ask for and get limited information from AOL, such as subscriber identity, billing data and payment history.

Other times police request all such information, plus e-mail; the online 'handles' and names of people cataloged in members' 'buddy lists;' all files attached to e-mail; and all other information contained about the subscriber in the America Online databases.

To comply with the more extensive orders, experts say, AOL must hand over a great deal.

'They can get all information,' said Mark Rasch, a former federal prosecutor and vice president for cyber law at Global Integrity. 'They can get your credit card data and everything you've filed with them. They can get a record of what times you dialed in, where you dialed in from, how long you were online, what activities you were engaged in, what Web sites you visited, what chat sessions you were in and what you said there.'

Internet service companies are privy to everything their members do online. But ISPs vary greatly in their record-retention policies. Some ISPs may keep e-mail for two years or more. Others may delete them after a few weeks. And that will affect authorities' ability to get what they want in criminal investigations.

For instance, he said, companies that host Web sites often keep records of the numeric Internet addresses that hit their sites for years, yet only the visitor's ISP can disclose which subscriber is behind that number.

America Online spokesman Nicholas Graham said the company had no comment on law enforcement's growing interest in subscriber records.

LOAD-DATE: July 31, 2000

Copyright 2000 International Herald Tribune
International Herald Tribune (Neuilly-sur-Seine, France)

July 28, 2000, Friday

SECTION: Opinion; Pg. 10

LENGTH: 560 words

HEADLINE: Wiretapping in Cyberspace

BYLINE: New York Times Service

BODY:

Millions of people now log on to the Internet as naturally and frequently as they pick up a phone. Technology has created a revolution in personal communications, but technology is also making it possible for government and even employers to monitor private conversations as never before. Telephone-era laws must be updated to address these new challenges to privacy.

Last week the White House proposed some limited changes to theU.S. wiretap and electronic privacy laws that would raise legal standards for government interception of e-mail. Separately, several lawmakersintroduced legislation to require employers to notify employees abouthow e-mail, Internet use and phone calls are monitored.

Employees of The New York Times Co. are already notified that the company reserves the right to reviewe-mail messages while investigating a complaint. Last year the company dismissed 23 employees - most based at a regional business office - for sending offensive e-mail messages.

In the absence of more stringent controls, law enforcement agencies may be tempted to conduct wholesale monitoring of digital written communications. New technology is making it possible for agencies like the FBI to scan, read and record millions of pieces of e-mail on the network of an Internet service provider. Until now this kind of power and its potential for abuse were not so readily available.

Current U.S. wiretapping laws were not drafted with this technology in mind and need to be updated. Various statutes now set different legal standards for the secret interception of domestic communications by law enforcement agencies, depending on whether the communication is by telephone, e-mail or cable modem. The Clinton administration is proposing to eliminate these inconsistencies. Its plan would bring the standards used for intercepting e-mail messages up to the stricter, more protective level now applied to telephone wiretaps. Illegal interception of e-mail would result in suppression of the evidence, as is the case now with illegal interception of phone calls.

The administration is also callingfor greater authority for courts to review law enforcement requests to use devices that record the phone numbers of incoming and outgoing calls and to track the origins and destinations of e-mail messages.

These changes are clearly needed. But Congress also needs to provide new safeguards against the government's wrongful use of ever more powerful surveillance technology against law-abiding citizens. Serious concerns have been raised about Carnivore, the new online wiretap system used by the FBI to track the communications of individuals suspected of criminal activity. The system, when hooked up to the network of the Internet service provider, gives the FBI unlimited access to the e-mail of all subscribers on the network. While a court order is still required to intercept the content of messages, the secret technology controlled exclusively by law enforcement raises fears

Doc. #55

of improper monitoring.

Until now, routine government surveillance of private conversations was limited as much by practicality as by legal constraints. Now that it is feasible to eavesdrop electronically on an unlimited scale, the laws have to be strengthened to prevent monitoring of all online communications simply because technology makes it easy.

LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC #8, OGC FRONT OFFICE FILE (PGS. 8 & 9)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #56 (Pages 812-813)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

FEDERAL BUREAU OF INVESTIGATION
OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS
WASHINGTON, D.C.

TO: MARCH TEL: _____

FAX: 703-632-6081

FROM: JAY TEL: _____

FAX: _____

DATE: 7/27

NO OF PAGES (EXCLUDING COVER): 4

CONTENTS/NOTE:

FYI

Doc. 57

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of Doc. #36 OPCA FILE 1 (PGS. 552-554)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #57, PGS. 2-4 (Pages 815 - 817)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc. #24, OGC FRONT OFFICE FILE (PAGE 15)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT # 58 (Page 818)

XXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

FBI

FUGITIVE PUBLICITY/ NATIONAL PRESS OFFICE

WASHINGTON, D.C.

TO: Marcus Thomas DATE: 7/25/00

ATTENTION:

FROM: [redacted] - OPCA

FACSIMILE #: _____ COMMERCIAL #: 202 [redacted]

64-1
67C-1

( ) URGENT (✓) HAND DELIVER ( ) ROUTINE

SUBJECT: This is a copy of what currently appears on the FBI website relative to Carnivore w/the exception of the graphic on the last page. [redacted] wrote an explanation ~~of the~~ for the graphic - we'd like to add it to the site.

COMMENTS:

If you have no problems w/this please initial & have faxed back to me. OR call - we can discuss. Thanks so much

NUMBER OF PAGES: _____ (Including cover page)

Tel: (202) 324-5348 Fax: (202) 324-3525 Homepage: http://www.fbi.gov

Doc. #59

CARNIVORE

Diagnostic Tool

Internet and Data Interception Capabilities Developed by the FBI, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. Donald M. Kerr

The Nation's communications networks are routinely used in the commission of serious criminal activities, including espionage. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities.

The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence -- not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,800 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques.

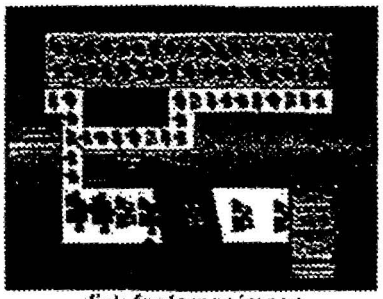
In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to

the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. This type of tool is necessary to meet the stringent requirements of the federal wiretapping statutes.

The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being transmitted either to or from the named subject.

Carnivore serves to limit the messages viewable by human eyes to those which are strictly included within the court order. ISP knowledge and assistance, as directed by court order, is required to install the device.



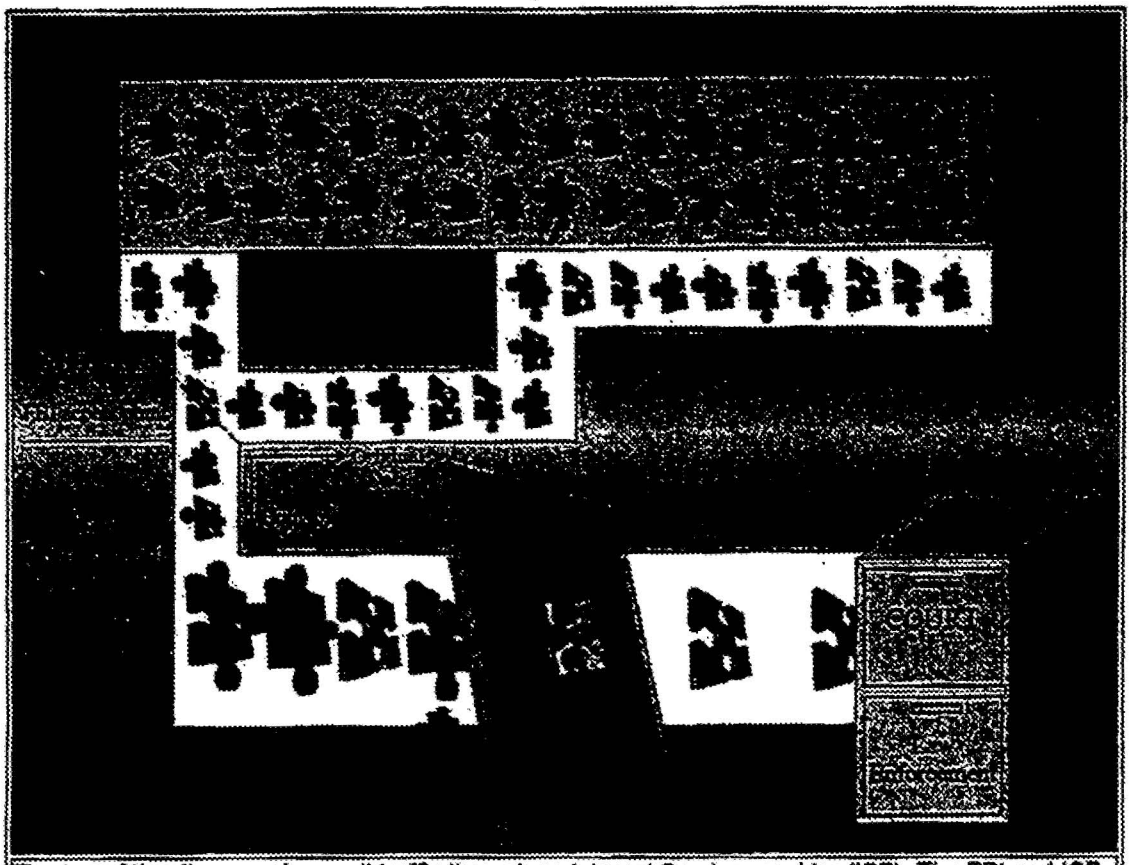
click for larger image

The use of the Carnivore system by the FBI is subject to intense oversight from internal FBI controls, the U. S. Department of Justice (both at a Headquarters level and at a U.S. Attorney's Office level), and by the Court. There are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties. The system is not susceptible to abuse because it requires expertise to install and operate, and such operations are conducted, as required in the court orders, with close cooperation with the ISPs.

The FBI is sharing information regarding Carnivore with industry at this time to assist them in their efforts to develop open standards for complying with wiretap requirements. The FBI did so two weeks ago, at the request of the Communications Assistance for Law Enforcement Act (CALEA) Implementation Section, at an industry standards meeting (the Joint Experts Meeting) which was set up in response to an FCC suggestion to develop standards for Internet interception.

This is a matter of employing new technology to lawfully obtain important information while providing enhanced privacy protection.

Programs and Initiatives | FBI Home Page



The top of the diagram shows all traffic through an Internet Service provider (ISP). The FBI and ISP work together to identify an access point that contains all traffic from the suspect named in the court order, with as little other traffic as possible. In some cases, the ISP is able to provide the FBI with an access point that contains only the suspect's traffic.

The FBI connects a commercially available one-way tapping device at the ISP's access point. This tap produces an exact copy of all data at the access point. The tap also provides electrical isolation to prevent Carnivore from having any kind of impact on the ISP's network.

The copied network traffic then flows into the collection system where it is compared against a predefined filter. This filter only passes traffic authorized for capture by the court order. Traffic that passes through the filter continues on to be archived to permanent storage media. No other data is ever stored to permanent media, nor is any information recorded about traffic that does not match the filters.

All information available to FBI case agents is also made available to the defense attorneys during the discovery process. In addition, all data stored to permanent media is sealed by the court that issued the court order. In response to a challenge, a judge can order the data to be unsealed and independently analyzed.

Carnivore	Programs and Initiatives	FBI Home Page

To: Finance From: Laboratory
Re: (U) [redacted] (S) 03/07/2000

ECE116, for an amount not to exceed $200,000, and [redacted] (S)

(U) Derived From : G-3
Declassify On: X1

Enclosure(s): (U) Requisition Number 858011.

Details: (U) The Data Intercept Technology Unit, EST-4, is responsible for creating the FBI's Internet intercept devices [redacted] (S) in support of field investigations. An integral part of supporting these collections and capabilities is operational tasking in support of (S) on going and pending [redacted] DRAGONET, [redacted] (S)

b1

(S) [redacted] (S)

TABLE 1: Proposed Funded Amounts by Program

PROGRAM	AMOUNT
[redacted] (S)	[redacted] (S)
DRAGONET	$200,000
[redacted] (S)	[redacted] (S)
[redacted] (S)	[redacted] (S)
TOTAL	[redacted] (S)

(Rev. 10-01-1999)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/07/2000

To: Finance

National Security

Laboratory

Attn: [redacted] Room [redacted]
[redacted] Room [redacted]
(Enclosure)
[redacted] Room [redacted]
[redacted] Room [redacted]
Room [redacted]
(enclosure)
Mr. McDevitt, Qt ERF
Mr. Thomas, QT ERF
[redacted] QT ERF
[redacted] QT ERF
[redacted] QT ERF
[redacted] QT ERF
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)

b6-1
b7C-1

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: Laboratory
Electronic Surveuillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

b6-1
b7C-1

Approved By: Kerr Donald M
Allen Edward L
McDevitt Michael J
Thomas Marcus C

MAR 2 9 2000
CLASSIFIED BY: AUC39677 SAH/cH
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

Drafted By: [redacted] llp

b6-1
b7C-1

Case ID #: ~~X~~ [redacted] (S)

Title: ~~X~~ [redacted] (S)

b1

Synopsis: ~~X~~ To request that the Contract Review Unit (CRU) approve and initiate an interim contract [redacted] for a [redacted] This tasking is to be funded under [redacted] BI number JVVCR1

(S)

b1
b4-1

~~SECRET~~

Doc. #60

b1 To: Finance From: Laboratory
Re: [redacted] 03/07/2000

(S) [redacted]

(U) DRAGONET is the program responsible for reactively developing Internet intercept capabilities and developing the capabilities to process the collected data. The sub tasking in this interim contract will include the following: 1) CARNIVORE developments, and 2) Communication protocol developments.

(S) [redacted]

b1 (S) [redacted] and, 2) the [redacted] The processing and modifications will include but not be limited to the exploration of utilizing a standalone data recording on the [redacted] that allows full system configuration.

(U) Requisition number 858011 is available for this procurement action and funding is available under [redacted] BI number JVVCRP, ECE116 for an amount not to exceed $200,000. [redacted]

(U) The EST-4 and EST-5 program areas as described above would like to request the that the Engineering Contracts Unit (ECU) approve and initiate an interim contract to be awarded b4-1 [redacted] and issue a purchase order for [redacted] b1 for the tasking as described in this memo. This matter has been coordinated with [redacted] NS-5A and b6-1 [redacted] NS-5B. b7C-1

To: Finance From: Laboratory
Re: (X) [redacted] (S) 03/07/2000

61

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

64-1 61 (X) (U) That the CRU initiate an interim contract to [redacted] (S) in support of the [redacted] (S) 61 DRAGONET, and [redacted] (S) programs.

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

(Rev. 10-01-1999)

on sent 4

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/15/2000

To: Finance

Criminal Investigative Laboratory

Attn: [redacted] Room [redacted]
[redacted] Room [redacted]
(Enclosure)
[redacted] Room [redacted]
Mr. McDevitt, QT ERF
Mr. Thomas, QT ERF
[redacted] QT ERF
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

66-1
67C-1

From: Laboratory
Electronic Surveillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

66-1
67C-1

Approved By: Kerr Donald M
Allen Edward L
McDevitt Michael J
Thomas Marcus C

MAR 20 2000 AUC 39677
CLASSIFIED BY: SAH/CH
REASON: 1.5 (e,g)
DECLASSIFY ON: X

Drafted By: [redacted] llp

66-1
67C-1

Case ID #: (X) [redacted] (S) 61
268-HQ-1092598 (Pending)

Title: (X) [redacted] (S) / DRAGONNET 61

Synopsis: (X) The Data Intercept Technology Unit (DITU) is requesting that the Contract Review Unit (CRU) add [redacted] (S) to [redacted] contract presently being negotiated. This funding is to support development efforts for lawfully authorized Title III Internet Collections. This tasking is to be funded under [redacted] (S)

64-1

61

61

SECRET

Doc #61

To: Finance From: Laboratory
Re: (S) [redacted] 03/15/2000

b1

[redacted] (S)

(U) ~~Derived From~~ : G-3
~~Declassify On~~: X1

Enclosure(s): (U) Requisition Number 858017.

Details: (S) The Data Intercept Technology Unit, EST-4, is responsible for creating the FBI's Internet intercept devices [redacted] (S) in support of field investigations. An integral part of supporting these collections and capabilities is operational tasking in support of on going and pending [redacted] DRAGONET, [redacted] (S)

(S) [redacted] (S)

b1

(S) [redacted] (S)

TABLE 1: Proposed Funded Amounts by Program

PROGRAM	AMOUNT
[redacted] (S)	[redacted] (S)
DRAGONET	$200,000
[redacted] (S)	[redacted] (S)

To: Finance From: Laboratory
Re: [redacted] 03/15/2000

b1

[redacted]	[redacted]
TOTAL	[redacted]

(S) [redacted]

(S) [redacted]

(S) [redacted]

(S) [redacted] and, 2) the [redacted] The augmentation of operational support for the processing and modifications will include but not be limited to the exploration of utilizing a standalone data recording on the [redacted] that allows full system configuration.

(X) Requisition number 858011 is available for this procurement action and funding is available [redacted]

(X) The EST-4 and EST-5 program areas as described above would like to request the that the Engineering Contracts

SECRET

To: Finance From: Laboratory
Re: [redacted] 03/15/2000

Unit (ECU) approve and initiate an interim contract to be awarded [redacted] and issue a purchase order for [redacted] for the tasking as described in this memo. This matter has been coordinated with [redacted] NS-5A and [redacted] NS-5B.

SECRET

5/24/02 Release - Page 830

SECRET

To: Finance From: Laboratory
Re: (X) [redacted] 03/15/2000

61

(S)

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

64-1 [redacted] (X) That the CRU initiate an interim contract to for [redacted] in support of the [redacted] DRAGONET, and [redacted] programs.

(S) 61 (S) 61 (S)

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

SECRET

5/24/02 Release - Page 831

(Rev. 10-01-1999)

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/15/2000

To: Finance

Attn: [redacted] Room [redacted]
Room [redacted]
(Enclosure)
[redacted] Room [redacted]
Room [redacted]
Room [redacted]
(enclosure)
QT ERF
QT ERF
QT ERF
QT ERF
QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)

National Security

Laboratory

66-1
67C-1

'ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: Laboratory
Electronic Surveuillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted] 66-1 67C-1

Approved By: Kerr Donald M
Allen Edward L
McDevitt Michael J
Thomas Marcus C

11-15-2000 AUC 39677
CLASSIFIED BY: SAH/SKS/cm
REASON: 1.5 (c,g)
DECLASSIFY ON: X 1
CV 01849

Drafted By: [redacted] llp 66-1 67C-1

Case ID #: X [redacted] (S) 61

Title: X [redacted] (S) 61

Synopsis: (U) To request that the Contract Review Unit (CRU) approve and initiate an interim contract with [redacted] for a 64-1

(U) ~~Derived From~~ : G-3
~~Declassify On~~: X1

SECRET

DOC #62

To: Finance From: Laboratory
Re: (U) [redacted] 03/15/2000

[redacted] This tasking is to be funded under [redacted] BI number JVVCRP, ECE116, for an amount not to exceed $200,000, and [redacted]

Enclosure(s): (U) Requisition Number 858011.

Details: (U) The Data Intercept Technology Unit, EST-4, is responsible for creating the FBI's Internet intercept devices [redacted] in support of field investigations. An integral part of supporting these collections and capabilities is operational tasking in support of on going and pending [redacted] DRAGONET, [redacted]

(S) [redacted]

TABLE 1: Proposed Funded Amounts by Program

PROGRAM	AMOUNT
[redacted]	[redacted]
DRAGONET	$200,000
[redacted]	[redacted]
[redacted]	[redacted]
TOTAL	[redacted]

To: Finance From: Laboratory
Re: (U) [redacted] 03/15/2000

(S) [redacted]

(U) DRAGONET is the program responsible for reactively developing internet intercept capabilities and developing the capabilities to process the collected data. The sub tasking in this interim contract will include the following: 1) CARNIVORE developments, and 2) Communication protocol developments.

(S) [redacted]

(S) [redacted] and, 2) the [redacted] augmentation of operational support for the [redacted] The processing and modifications will include but not be limited to the exploration of utilizing a standalone data recording on the [redacted] that allows full system configuration.

(U) Requisition number 858011 is available for this procurement action and funding is available [redacted] BI number JVVCRP, ECE116 for an amount not to exceed $200,000, [redacted]

(U) The EST-4 and EST-5 program areas as described above would like to request the that the Engineering Contracts Unit (ECU) approve and initiate an interim contract to be awarded [redacted] and issue a purchase order for [redacted] for the tasking as described in this memo. This matter has been coordinated with [redacted] NS-5A and [redacted] NS-5B.

To: Finance From: Laboratory 61
Re: [redacted] (S) 03/15/2000

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

64-1 [redacted] That the CRU initiate an interim contract to for [redacted] (S) in support of the [redacted] (S) DRAGONET, and [redacted] programs.

61

Set Lead 2: 61

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

5/24/02 Release - Page 835

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

18 Page(s) withheld for the following reason(s): PREVIOUSLY PROVIDED TO PLAINTIFF AS PART OF RELEASE #3

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #63 STATEMENT OF WORK DATED MARCH 23, 2000

(Pages 836-853)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

(Rev. 10-01-1999)

Desk 27

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/24/2000

To: Finance

Attn: [redacted] Rm [redacted]
[redacted] Rm [redacted]
(enclosures)

Laboratory

Mr. Thomas, QT ERF
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosures)
[redacted], QT ERF
(enclosures)
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosures)
[redacted]
(enclosures)

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

66-1
67C-1

From: Laboratory
Electronic Surveillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

66-1
67C-1

DRAFT

Approved By: Allen Edward L
McDevitt Michael J
Thomas Marcus C
[redacted]

66-1
67C-1

Drafted By: [redacted] llp

Case ID #: (X) [redacted] (S) / 268-HQ-1092598 61

Title: (X) [redacted] (S) / DRAGONET 61

Synopsis: (U) To request that the Contract Review Unit (CRU) modify the existing FY2000 contract with [redacted] and issue a purchase order for a total amount of $1,045,000. 64-1

(U) ~~**Derived From :** G-3~~
~~**Declassify On:** X1~~

Enclosure(s): (U) 1) Requisition number 858017 for $1,045,000,

SECRET

8-24-00 AUC39677
CLASSIFIED BY: SAH | JS | CH
REASON: 1.5 (9)
DECLASSIFY ON: X 1

DOC #64

To: Finance From: Laboratory
Re: [redacted] 03/24/2000

Details: (U) The DRAGONET Program is the FBI Title III Internet intercept program. This program is responsible for developing the capability of supporting lawfully authorized Internet packet captures in support of law enforcement requirements. This highly specialized collection technology has been developed [redacted] under the codename CARNIVORE. To support the CARNIVORE system which can intercept this traffic is needed. To reduce the cost of this effort, a modification to the [redacted] system will be made. The [redacted] system was originally developed for the [redacted] program and has the capabilities needed by the Dragonet program.

(U) the DRAGONET program is also developing ???(700K)

(U) The Threat Analysis Program has a need for continuing [redacted] support. [redacted] has provided and is supporting an operational database that tracks field operations for EST-4, EST-5, NSD, and the field. The continued operation of this database is critical to operational ERF and field personnel.

(U) A new contract is currently being negotiated with [redacted] for Fiscal year 2000. Please reference electronic communication, titled [redacted] Contract initiation", and dated 11/10/99 for the details of this new contract. The tasking's and funding detailed in the EC is for funding under this new contract.

(U) EST-4 would like to request additional FY2000 funding be transferred to [redacted] to address the following three program areas as delineated in the following table and detailed below.

(U) TABLE 1: Funding Amount By Program

PROGRAM AREA	AMOUNT
1.0 Dragonet - [redacted] Production	$320,000
2.0 Dragonet - ??	$700,000
3.0 Threat Analysis Program	$25,000
TOTAL	$1,045,000

To: Finance From: Laboratory
Re: (X) [redacted] (S) 03/24/2000

(U) Task 1.0 DRAGONET Program Funding - [redacted] (S) PROCUREMENT:

61

(S) Dragonet has an immediate need for the production of the [redacted] (S)

(X) The contractor shall provide a cost estimate for the production of [redacted] (S)

(U) Task 2.0 DRAGONET Program - ???

(U) Task 3.0 Threat Analysis Program

(U) The contractor shall provide software upgrade installation support and software maintenance for the Technical Threat Analysis database and the Special Projects database. The contractor shall supply a software engineer, with an anticipated minimum level of EL-4, to support this effort at a rate of twenty five(25) hours per month.

(U) LOCATION OF WORK

(U) Due to space limitations in the Engineering Research Facility (ERF), it will not be possible to perform all services at the ERF's facility. Accordingly, the Contractor must be prepared to conduct operations in an external location selected by them. FBI reserves the right to approve any such external facilities should a contingency arise.

IX. (U) GOVERNMENT FURNISHED EQUIPMENT

(U) The Government will furnish hardware, applicable documentation and additional GFE requirements that should be identified by the contractor in his proposals.

X. (U) PROGRAM MANAGEMENT

To: Finance From: Laboratory 61
Re: [redacted] 03/24/2000

(S)

(U) To provide managerial and administrative support for the FBI's programs. Scheduling, task assignments and budgets shall be generated. Monthly status reports and other relevant FBI Program Management Office (PMO) documentation shall be [redacted] applied to the FBI Contracting Officer's Technical Representative (COTR) at required intervals. These reports are to include monthly progress during the previous period and expected progress for the following monthly period. Budgeting information, including expenditures to date is to be provided to the FBI on a monthly basis. As part of the contractors program management responsibilities, the contractor shall inform the FBI's Contracting Officer (CO) and Contracting Officer's Technical Representative (COTR), in writing, when any of the tasks reach a seventy percent (70%) spending level. The contractor shall also provide a cost analysis of the remaining funds and time requirements that show the remaining funds are sufficient or insufficient for completing the task.

SECRET

61

To: Finance From: Laboratory
Re: (U) [redacted] 03/24/2000

(5)

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

64-1 (U) That the ECU increase the funding for the FY 2000 [redacted] contract by $1,045,000 for fiscal year 2000, in support of the Dragonet and Technical Threat Analysis programs.

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

SECRET

5/24/02 Release - Page 858

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

20 Page(s) withheld for the following reason(s): PREVIOUSLY PROVIDED TO PLAINTIFF AS PART OF RELEASE #3

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #65, STATEMENT OF WORK DATED MARCH 24, 2000
(Pages 859-878)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

on. 01/3/01

SECRET

STATEMENT OF WORK

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

(U) STATEMENT OF WORK FOR FY 2000

(ADDITIONAL TASKING)

b4-1 [redacted]

b1 [redacted] (S)

DRAGONET THREAT ANALYSIS PROGRAM

June 1, 2000

MAR 2 0 2001 AUC 39677
CLASSIFIED BY: SAH/CH
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

(U) ~~Derived From : G-3~~
~~Declassify On: X1~~

SECRET

Doc. #66

STATEMENT OF WORK [redacted]

b4-1

TABLE OF CONTENTS

SECTION	TITLE	PAGE
I.	(U) INTRODUCTION	3
II.	(U) PROJECT DESCRIPTION BY TASKING AREAS	3
III.	(U) TASKING AREA #2.8 - RENAMING TASK	3
IV.	(U) TASKING AREA #2.14 - [redacted]	3
V.	(U) TASKING AREA #4.3 - DRAGONET - [redacted]	4
VI.	(U) TASKING AREA #4.4 - DRAGONET - HIGH SPEED INTERCEPT STUDY	4
VII.	(U) TASKING AREA #6.0 - THREAT ANALYSIS PROGRAM	4
VIII	(U) LOCATION OF WORK	4
IX.	(U) GOVERNMENT FURNISHED EQUIPMENT	4
X.	(U) Program Management	5

b1 (5) (5) b1

STATEMENT OF WORK

I. (U) INTRODUCTION

64-1 61

(S) [redacted] has been and is currently being tasked with [redacted] software and [redacted] This SOW will incorporate additional tasking and tasking modifications for the current FY 2000 contract J-FBI-00-080. (S)

II. (U) PROJECT DESCRIPTION BY TASKING AREAS

64-1

(U) The [redacted] tasking (Tasking numbers are referenced to the original contract tasks):

64-1

(U) TABLE 1: [redacted] Tasking Area Summary Table

TASKING AREA #	TASK DESCRIPTION
2.8	RENAMING TASK
2.14	(S) [redacted] TASKING
4.3	DRAGONET - [redacted] (S)
4.4	DRAGONET - High Speed Intercept Study
6.0	Technical Threat Analysis Program - Data Base Support

61

(U) Sections III, IV, V, VI, and VII give a more detailed description of the tasking for FY2000.

III. (U) TASKING 2.8 - HAWKING ROUTER ENHANCEMENTS :

(U) This task has been renamed **VIKING ENHANCEMENTS.**

61

IV (U) TASKING 2.14 - [redacted] (S) TASKING :

61

(S) [redacted] (S)

V. (U) TASKING AREA #4.3 - [redacted] (S)

b1

[redacted]

VI. (U) TASKING AREA #4.4 HIGH SPEED INTERCEPT STUDY

b1 (S) [redacted] This task shall provide the DRAGONET program with a capability for Internet data interception. The contractor shall make enhancements to existing Carnivore intercept drive overall system throughput performance. These enhancements will make use operating system performance enhancements to include service pack 1 with additional capability that will be added in addition to overall throughp Carnivore to filter on PPP streams and the update of the graphical user filter associated with PPP.

VII. (U) THREAT ANALYSIS PROGRAM

STATEMENT OF WORK

(U) The contractor shall provide software upgrade installation support and software maintenance support for the Technical Threat Analysis database and the Special Projects database. The contractor shall supply a software engineer, with an anticipated minimum level of EL-4, to support this effort at a rate of twenty five (25) hours per month.

VIII. (U) LOCATION OF WORK

(U) Due to space limitations in the Engineering Research Facility (ERF), it will not be possible to perform all services at the ERF's facility. Accordingly, the Contractor must be prepared to conduct operations in an external location selected by them. FBI reserves the right to approve any such external facilities should a contingency arise.

IX. (U) GOVERNMENT FURNISHED EQUIPMENT

(U) The Government will furnish hardware, applicable documentation and additional GFE requirements that should be identified by the contractor in his proposals.

X. (U) PROGRAM MANAGEMENT

(U) To provide managerial and administrative support for the FBI's programs. Scheduling, task assignments and budgets shall be generated. Monthly status reports and other relevant FBI Program Management Office (PMO) documentation shall be generated and supplied to the FBI Contracting Officer's Technical Representative (COTR) at required intervals. These reports are to include monthly progress during the previous period and expected progress for the following monthly period. Budgeting information, including expenditures to date is to be provided to the FBI on a monthly basis. As part of the contractors program management responsibilities, the contractor shall inform the FBI's Contracting Officer (CO) and Contracting Officer's Technical Representative (COTR), in writing, when any of the tasks reach a seventy percent (70%) spending level. The contractor shall also provide a cost analysis of the remaining funds and time requirements that show the remaining funds are

sufficient or insufficient for completing the task.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

4 Page(s) withheld for the following reason(s): RESPONSIVE PAGES FROM THIS REPORT WERE PART OF RELEASE #5

☒ The following number is to be used for reference regarding these pages:
DOCUMENT 67, FY 2000 TECHNICAL PROPOSAL
(Pages 885-888)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

(Rev. 10-01-1999)

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/16/2000

To: Finance **Attn:** Mr. Stollhans, Room 6032
[redacted] Room [redacted]
(Enclosure)
[redacted] Room [redacted]
(Enclosure)
Mr. Thomas, QT ERF
[redacted] QT ERF
[redacted] QT ERF
[redacted] QT ERF
(Enclosure)

Criminal Investigative 66-1
Laboratory 67C-1

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: Laboratory
Cyber Technology Section,
Data Intercept Technology Unit, QT ERF
Contact: SSA [redacted] (703) [redacted] 66-1 67C-1

Approved By: Kerr Donald M
Allen Edward
Thomas Marcus
[redacted]

Drafted By: [redacted] llp 4047 ... 66-1 67C-1

Case ID #: 268-HQ-1092598 (Pending)

Title: DRAGONNET

Synopsis: Request of the Finance Division to assign funding for requisition number 827303 from budget line item ETX122, in the amount of $347,730, modifying contract J-FBI-00-080 [redacted] Inc. 64-1

Enclosure(s): Enclosed for Finance is Requisition number 827303.

Details: Requisition number 827303 is being submitted to modify the existing contract number J-FBI-00-080, [redacted] The modification consists of increasing the original contract by $347,730. The additional funding will provide for one Senior Engineer, for a one year period, to support deployment of Internet Interception and Collection systems. This task will consist of supporting system deployments [redacted] 64-1

61

(S)

MAR 20 2002

CLASSIFIED BY: AUC 39677 SAH/cdl
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

SECRET

Doc. #68

SECRET

This modification will also provide additional funds to the operational support task [redacted] (S)

b1

The Contracting Officer is [redacted] Program Leader is [redacted] The COTR is [redacted]

b6-1
b7C-1

SECRET

5/24/02 Release - Page 890

~~SECRET~~

LEAD(s):

Set Lead 1 (Adm)

FINANCE

AT WASHINGTON, DC

The Finance Division is requested to modify Contract Number J-FBI-00-080.

Set Lead 2 (Adm)

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

64-1 To approve funding for requisition number 827303 from budget line item ETX122, in the amount of $347,730, modifying contract J-FBI-00-080 [redacted]

Set Lead 3 (Adm)

LABORATORY

AT QUANTICO, VA

For information only.

♦♦

~~SECRET~~

5/24/02 Release - Page 891

DRAFT

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

SECRET

[redacted] (FOUO) (S)

[redacted] (FOUO) (S)

[redacted] (FOUO) (S)

61

[redacted] (FOUO) (S)

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

SECRET

5/24/02 Release - Page 89

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

~~SECRET~~

DRAFT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

- Should be in the form of a memo from the Director to the AG. May 5, 2000
- Should be classified ~~SECRET~~.
- Has NSLU reviewed?

MAR 2 0 2002

AUC 39677

CLASSIFIED BY: SAHlcb
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (FOUO)

[redacted] (S)

b1

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

~~SECRET~~

Doc. #69

DRAFT

SECRET

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

[redacted] (S)

[redacted] (S)

Proposed Procedures:

[redacted] (S)

[redacted] (S)

[redacted] (S)

b1

3. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (Fouo) (4)

[redacted] (S)

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

SECRET

5/24/02 Release - Page 89

DRAFT

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

b1 [redacted] (FOUO) (S)

[redacted] (FOUO) (S)

6. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General ~~or designee of the Attorney General~~. ~~(FOUO)~~ (U)

7. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. ~~(FOUO)~~ (U)

8. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

b1 [redacted] (S)

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

~~SECRET~~

5/24/02 Release - Page 895

SECRET

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

May 12, 2000

MAR 20 2002 AUC 39677
CLASSIFIED BY: SAH/CA
REASON: 1.5 (c,g)
DECLASSIFY ON: X1

Director:

b1

(S) [redacted] (S)

(S) [redacted] (S)

(X) After recognizing the efficacy of using these statutorily-based procedures, the LD shared this proposed course of action with the Counterterrorism Division and the Office of the General Counsel, and they acknowledged the usefulness of this (U)

Enclosures (2)

b6-1
b7C-1

1 - Mr. Pickard, Room 7142
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted], Room 7427
ARM:pak (17)

1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Dr. Kerr, Room 3090
1 - Mr. Allen, QT ERF
1 - Mr. Thomas, QT ERF
1 - [redacted] QT ERF
1 - [redacted] Room [redacted]

(U) ~~Classified by: G-3~~
~~Declassify on: X-1~~

SECRET

Doc. #70

approach. Moreover, the LD has shared with the DOJ's Office of Intelligence Policy and Review (OIPR) a draft of the attached proposed memorandum to the Attorney General, which includes the proposed electronic surveillance testing procedures. OIPR supports this "testing" approach, as provided for in the FISA [redacted] and it also supports the specific testing procedures proposed by the LD. (U) (See attachment #2).

b1

[redacted] (S)

~~(FOUO)~~ If you approve of this approach, the OIPR advises that the FBI request should be forwarded to the Attorney General through the attached memorandum, which the OIPR has already approved in draft form. (U)

Donald M. Kerr

5/24/02 Release - Page 897

[redacted]

ATTACHMENT 1

SECRET

Memorandum

To : Mrs. Frances Fragos Townsend Date 04/28/2000
Counsel, Office of Intelligence
Policy and Review

From : Dale L. Watson
Assistant Director
Counterterrorism Division

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Subject : [redacted] (S)

b1

ACTION MEMORANDUM

(S) [redacted]

(S)

b1

[redacted]

(S) The Carnivore software filters the target's communications from other communications and stores the targeted communications to storage media where the communications can be maintained as evidence.

1 - [redacted]
1 -
1 -
1 -
1 -
1 -
1 -
AMK:amk(8)

b6-1
b7C-1

SEE NOTE PAGE FIVE

Classified by: 4877, ITOS, CTD
Reason: 1.5(C)
Declassify on: X1

MAR 2 9 2002

SECRET

AUC 39677
CLASSIFIED BY: SAH\cdh
REASON: 1.5 (c,g)
DECLASSIFY ON: X 1

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review
Re: [redacted] (S) b1

[redacted] (S)

(U) The Carnivore software has been developed and tested over a period of years and has been deployed in the field successfully on numerous occasions. However, it has never been installed in the USA.NET network. While most networks use standard protocols, protocols can vary widely from the standards in some networks.

b1

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

5/24/02 Release - Page 900

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review

Re: [redacted] (S) b1

b1

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

5/24/02 Release - Page 001

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review

Re: [redacted] (S)

61

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

5/24/02 Release - Page 902

SECRET

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review
Re: [redacted] (S)

b1

[redacted] (S)

SECRET

5/24/02 Release - Page 903

[redacted]

ATTACHMENT 2

SECRET

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

EXECUTIVE SUMMARY

TO: THE ATTORNEY GENERAL

THROUGH: MRS. FRANCES FRAGOS TOWNSEND
COUNSEL, OFFICE OF INTELLIGENCE
POLICY AND REVIEW

FROM: LOUIS J. FREEH
DIRECTOR, FBI

SUBJECT: (U) REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

PURPOSE: (U) To obtain the Attorney General's approval of the attached FBI electronic surveillance testing procedures pursuant to authority vested in the Attorney General in Section 105(f) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. 1805(f).

TIMETABLE: (X) The Attorney General is requested to approve the proposed FBI testing procedures as soon as possible. Testing pursuant to these procedures is essential for the FBI to be able(w)

Classified by: G-3
Declassify on: X-1

MAR 2 0 2002 AUC 59677
CLASSIFIED BY: SAM/CL
REASON: 1.5 (C,G)
DECLASSIFY ON: X 1

SECRET

SECRET

Memorandum to The Attorney General from Director, FBI

[redacted] (S)

b1

[redacted] (S)

RECOMMENDATION: (U) Attorney General approve the attached FBI electronic surveillance testing procedures.

APPROVE _____

DISAPPROVE _____

OTHER _____

Concurring components:

NONE

Nonconcurring components:

NONE

SECRET

[redacted]

SECRET

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

MAR 2 0 2002 Auc 39677

CLASSIFIED BY: SAH\CH
REASON: 1.5 (c,g)
DECLASSIFY ON: X 1

MEMORANDUM FOR THE ATTORNEY GENERAL

THROUGH: MRS. FRANCES FRAGOS TOWNSEND
COUNSEL, OFFICE OF INTELLIGENCE
POLICY AND REVIEW

FROM: Louis J. Freeh
Director, FBI

SUBJECT: (U) REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

PURPOSE: (U) To obtain the Attorney General's approval of the attached FBI electronic surveillance testing procedures pursuant to authority vested in the Attorney General in Section 105(f) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. 1805(f).

TIMETABLE: (X) The Attorney General is requested to approve the proposed FBI testing procedures as soon as possible. Testing pursuant to these procedures is essential for the FBI [redacted] (S)

61 [redacted] (S)

(U) Classified by: G-3
Declassify on: X-1

SECRET

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

[redacted] (S)

[redacted] (S)

b1

[redacted] (S)

5/24/02 Release - Page 90

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

[redacted] (S)

[redacted] (S)

b1

[redacted] (S)

[redacted] (S)

5/24/02 Release - Page 909

b1

[redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

[redacted] (S)

~~(TOUO)~~ Proposed Procedures:

(S) [redacted] (S)

(S) [redacted] (S)

(X) 2. [redacted] (S)

b1

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

b1 [redacted] (S) Carnivore is an FBI-designed software program that, in important respects, filters and then intercepts with great precision various ISP data elements (including content when authorized) based upon reference to certain standardized ISP TCP/IP protocols.

b1 (S) [redacted] (S)

~~(FOUO)~~ 4. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (4)

b1 [redacted] (S)

b1 [redacted] (S)

~~(FOUO)~~ 7. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General. (4)

~~(FOUO)~~ 8. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. (4)

5/24/02 Release - Page 912

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

~~(FOUO)~~ 9. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

RECOMMENDATION: Attorney General approve the attached electronic surveillance testing procedures. (U)

APPROVE _____

DISAPPROVE _____

OTHER _____

Concurring components:

NONE

Nonconcurring components:

NONE

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

66-1
67C-1

1 - Mr. Pickard, Room 7142
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Mr. Parkinson, Room 7427
PAK (17)

1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Dr. Kerr, Room 3090
1 - Mr. Allen, QT ERF
1 - Mr. Thomas, QT ERF
1 - [redacted] Room [redacted]
1 - [redacted] QT ERF

5/24/02 Release - Page 914

SECRET

Memorandum

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

To : The Attorney General Date 05/11/2000

From : Director, FBI

Subject : (U) REQUEST FOR APPROVAL OF TESTING OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

b1

(S) [redacted] (S)

(S) [redacted] (S)

[redacted] (S)

MAR 2 0 20[redacted] AUC 39677
CLASSIFIED BY: SAH/cH
REASON: 1.5 (a) (1)
DECLASSIFY ON: [redacted]

SECRET

Doc # 71

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

b1

5/24/02 Release - Page 916

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

[redacted] (b)

[redacted] (b)

b1

5/24/02 Release - Page 917

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

(S) [redacted] (S)

(S) [redacted] (S)

b1

~~(FOUO)~~ Proposed Procedures:

(S) [redacted] (S)

5/24/02 Release - Page 918

(S) [redacted] (S)

(X) 2. Testing Equipment: [redacted] (S) Carnivore is an FBI-designed software program that, in important respects, filters and then intercepts with great precision various ISP data elements (including content when authorized) based upon reference to certain standardized ISP TCP/IP protocols.

b1

(S) [redacted] (S)

~~(FOUO)~~ 4. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (U)

[redacted] (S)

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

b1

[redacted] (S)

[redacted] (S)

~~(FOUO)~~ 7. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General. (U)

~~(FOUO)~~ 8. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. (U)

~~(FOUO)~~ 9. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

5/24/02 Release - Page 220

SECRET

MEMORANDUM FOR THE ATTORNEY GENERAL 6/1/00

THROUGH: MRS. FRANCES FRAGOS TOWNSEND
COUNSEL, OFFICE OF INTELLIGENCE
POLICY AND REVIEW

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

FROM: LOUIS J. FREEH
DIRECTOR, FBI

SUBJECT: (U) REQUEST FOR APPROVAL OF TESTING OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

PURPOSE: (U) To obtain the Attorney General's approval of the attached FBI electronic surveillance testing procedures pursuant to authority vested in the Attorney General in Section 105(f) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. 1805(f).

TIMETABLE: (S) The Attorney General is requested to approve the proposed FBI testing procedures as soon as possible. Testing pursuant to these procedures is essential for the FBI [redacted] (S)

61

[redacted] (S)

66F-HQ-1012493

66-1
67C-1

1 - Mr. Pickard, Room 7142
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Mr. Parkinson, Room 7427
ARM:pak (17)

1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Dr. Kerr, Room 3090
1 - Mr. Allen, QT ERF
1 - Mr. Thomas, QT ERF
1 - [redacted] Room [redacted]
1 - [redacted] QT ERF

(U) ~~Classified by: G-3~~
~~Declassify on: X-1~~

SECRET

5/24/02 Release - Page 92

3-20-02 AMC 39677
CLASSIFIED BY: SA #1 cd
REASON: 1.5 (c, g)
DECLASSIFY ON: X 1

Doc #72

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

b1

[redacted] (S)

[redacted] (S)

[redacted] (S)

5/24/02 Release - Page 922

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

b1

5/24/02 Release - Page 923

[redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

b1

[redacted]

(S)

~~(FOUO)~~ Proposed Procedures:

(S) [redacted]

(S)

(S) [redacted]

(S)

(S) 2. [redacted]

(S)

b1

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

[redacted] (S) Carnivore is an FBI-designed software program that, in important respects, filters and then intercepts with great precision various ISP data elements (including content when authorized) based upon reference to certain standardized ISP TCP/IP protocols.

(S) [redacted] (S)

~~(FOUO)~~ 4. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (U)

b1

[redacted] (S)

[redacted] (S)

~~(FOUO)~~ 7. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General. (U)

~~(FOUO)~~ 8. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. (U)

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

~~(FOUO)~~ 9. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

RECOMMENDATION: Attorney General approve the attached electronic surveillance testing procedures. (U)

APPROVE _____

DISAPPROVE _____

OTHER _____

Concurring components:

NONE

Nonconcurring components:

NONE

5/24/02 Release - Page 927

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

5/24/02 Release - Page 92